Dr.WEB®

für Android

Defend what you create

Benutzerhandbuch

© Doctor Web, 2014. Alle Rechte vorbehalten

Das im vorliegenden Dokument enthaltene Material ist Eigentum von Doctor Web und dient ausschließlich der persönlichen Nutzung durch Produktkäufer. Kein Teil des vorliegenden Dokumentes dard ohne Quellenangabe weder reproduziert noch auf einer Netzwerkressource untergebracht oder mittels Kommunikationskanäle und Massenmedien verbreitet oder auf jede andere Weise benutzt werden, ausgenommen Nutzung für persönliche Zwecke.

WARENZEICHEN
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, Dr.Web AV-Desk, Dr.WEB Logos sind eingetragene Warenzeichen von Doctor Web in Russland und/oder anderen Ländern. Alle sonstigen eingetragenen Warenzeichen, Logos und Firmennamen, die im vorliegenden Dokument erwähnt sind, sind Eigentum ihrer jeweiligen Inhaber.

HAFTUNGSAUSSCHLUSS
Unter keinen Umständen haften Doctor Web und seine Lieferanten für die im vorliegenden Dokument enthaltenen Fehler und/oder Auslassungen sowie für Schäden des Produktkäufers (direkte oder indirekte Schäden einschließlich Gewinnausfälle), die sich dadurch ergeben.

Dr.Web antivirus für Android
Version 9.01.5
Benutzerhandbuch
18.09.2014

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Website: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Website

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie umfangreiche Geographie der Benutzer zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken den Benutzern für Unterstützung der Lösungen von Dr.Web-Familie!

Inhaltsverzeichnis

Kapitel 1. Einführung 6

Symbole und Abkürzungen 6

Hauptfunktionen 7

Kapitel 2. Lizenzierung 8

Lizenzschlüsseldatei 9

Schlüsseldatei erhalten 10

Schlüsseldatei verwenden 12

Lizenz verlängern 13

Kapitel 3. Installation und Deinstallation 15

Systemanforderungen 15

Programm installieren 15

Programm deinstallieren und aktualisieren 17

Kapitel 4. Mit der Arbeit beginnen 18

Antivirusprogramm starten und beenden 18

Oberfläche 18

Widgets 19

Benachrichtigungen 20

Mein Dr.Web 21

Kapitel 5. Programmfunktionen und -einstellungen 23

Virenschutz 25

Permanenter Virenschutz 25

Überprüfung auf Anforderung des Benutzers 26

Neutralisierung der Bedrohungen 28

Bedrohungen bei Systemanwendungen entdecken 29

Sperr-Software bearbeiten 29

Anruf- und Nachrichtenfilter 30

Filtermodus wählen 31

Blacklist 31

Filterprofil erstellen 32

Gesperrte Anrufe und Nachrichten einsehen 33

Virendatenbanken aktualisieren 34

Mit Quarantäne arbeiten 34

Statistik 35

Dr.Web Anti-Theft 36
Ersteinstellung 37
Optionen einstellen 39
Freundesliste 40
SMS-Befehle 41
Passwort wiederherstellen 42
Zugriff auf Internet-Inhalte einschränken 42
Dr.Web Firewall 43
Mobiles Internet einschränken 45
Anwendungsdatenverkehr behandeln 47
Aktuelle Aktivität der Netzwerkverbindungen 49
Ereignisse registrieren 50
Bei Beseitigung der Sicherheitslücken helfen 51
Betriebsmodus wählen 55
Kurz-URL-Dienst 57
Anhang 58
Anhang A. Technischer Support 58
Index 59

Kapitel 1. Einführung

Vielen Dank, dass Sie sich für **Dr.Web antivirus für Android** entschieden haben. Dieses Antivirenprodukt schützt mobile Geräte mit Android™-Betriebssystem zuverlässig vor unterschiedlichen Viren, die speziell zum Infizieren mobiler Geräte geschaffen wurden.

Im Programm wurden die meist fortgeschrittenen Konzepte und Technologien von **Doctor Web** eingesetzt, mit denen sich die Malware-Objekte, durch welche die Funktion und Informationssicherheit des Geräts gefährdet werden können, entdecken und desinfizieren lassen.

Dr.Web antivirus nutzt Origins Tracing™ for Android. Es ist die einzigartige Technologie zur Erkennung böswilliger Programme für Android-Plattform. Diese Technologie sorgt dafür, dass neue Virenfamilien aufgrund der schon bestehenden Kenntnisse über herkömmliche Bedrohungen entdeckt werden können. Mit Origins Tracing for Android lassen sich sowohl neu kompilierte Viren wie Android.SMSSend, Android.MobileSpy als auch die mit Android.ADRD, Android.Geinimi, Android.DreamExploid infizierten Anwendungen erkennen. Die mit Hilfe von Origins Tracing for Android entdeckten Bedrohungen erhalten den Namen Android.VirusName.origin.

In diesem Handbuch finden die Benutzer von mobilen Geräten die Anweisungen zur Installation und Konfiguration von **Dr.Web antivirus** sowie Informationen zu seinen Hauptfunktionen.

Symbole und Abkürzungen

In der Anleitung werden folgende Bezeichnungen verwendet:

Bezeichnung	Kommentar
Fette Schrift	Elemente einer grafischen Benutzeroberfläche und Beispiele für Eingaben, die man exakt durchführen muss, wie sie in der Anleitung stehen.
Grüner und fetter Duktus	Die Namen der **Doctor Web** Produkte oder deren Komponenten.
Grüner und unterstrichener Duktus	Links zu Hilfs- und Webseiten.
`Monoschrift`	Beispiele des Codes für die Kommandozeileneingabe und die Informationen, die an den Benutzer von der Anwendung ausgegeben wird.
Kursiv	Fachausdrücke und alternativer Text (wird statt Informationen geholt, die der Benutzer eingeben muss). Im Falle der Beispiele für die Kommandozeileneingabe wird kursiv auf die Parameterwerte anzeigen.
TITELBUCHSTABEN	Die Namen der Tasten auf der Tastatur.
	Wichtiger Hinweis oder eine Warnung vor potenziell gefährlichen oder folgenschweren Situationen.

Hauptfunktionen

Dr.Web antivirus ist eine zuverlässige Antivirenlösung für Benutzer von mobilen Geräten, die unter Android laufen. Die Anwendung realisiert folgende Funktionen:

- permanenter Echtzeitschutz des Dateisystems (Prüfung der zu speichernden Dateien, zu installierenden Programme u a.m.)
- Alle Dateien des Systems bzw. einzelne Dateien und Ordner auf Anforderung des Benutzers scannen
- Archive scannen
- Auf Speicherkarte scannen
- Windows-Autostart-Dateien entdecken
- Bedrohungen in .lnk-Dateien (durch **Dr.Web** als **Exploit.CplInk** definiert) entdecken
- Entdeckte Bedrohungen löschen bzw. in die Quarantäne verschieben
- Das Gerät bei seiner Blockierung durch Erpesser-Software freigeben
- Eingehende Anrufe und SMS-Nachrichten aufgrund der voreingestellten bzw. benutzerdefinierten White- und Blacklists filtern
- **Dr.Web Virendatenbanken** über Internet aktualisieren
- Statistiken über entdeckte Bedrohungen und Aktionen des Programms sowie Ereignislog führen
- Handy orten und sofort sperren, wenn es verloren geht oder gestohlen wird
- Vor unerwünschten Webinhalten bei Nutzung eines Standard-Android-Browsers sowie des Browsers Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser bzw. Boat Browser Mini schützen
- URL überprüfen und kürzen
- Sicherheitsprobleme und -lücken des mobilen Geräts aufdecken und beseitigen
- Internetverbindungen überwachen, das mobile Gerät vor unbefugtem Zugriff von außen schützen sowie dem Verlust wichtiger Daten im Netzwerk vorbeugen

Durch eine bequeme graphische Oberfläche lassen sich die Anwendungsparameter mit Rücksicht auf Bedürfnisse des Benutzers vollständig konfigurieren und ein optimales Schutzniveau für mobiles Endgerät einstellen.

Dr.Web antivirus kann auch im Multi-Window Modus genutzt werden. In diesem Modus lassen sich mehrere Anwendungen in einzelnen Fenstern starten. Der Multi-Window Modus wird nur von Samsung Galaxy S III und höher sowie Samsung Galaxy Note 2 und höher unterstützt.

Kapitel 2. Lizenzierung

Die Benutzerrechte zur Nutzung von **Dr.Web antivirus** werden mit Hilfe einer speziellen Datei geregelt, die *Schlüsseldatei* genannt wird.

Das Verfahren für den Kauf und die Registrierung der Lizenz für die Version **Dr.Web antivirus**, die über Google Play installiert werden kann, weicht von demjenigen für die Version, die von der Website von **Doctor Web** heruntergeladen und installiert werden kann, ab.

Wird für die Anwendungsversion die uneingeschränkte Lizenz (**Dr.Web Anti-virus Life license**) über Google Play erworben und installiert, wird die Lizenz automatisch erhalten und registriert.

Bei Aktivierung des zentral verwalteten Schutzmodus wird die Lizenz vom zentral verwalteten Virenschutz-Server automatisch heruntergeladen.

Wenn Sie eine gültige Lizenz für **Dr.Web® Security Space** oder **Dr.Web® Desktop Security Suite** oder beliebige handelsübliche, seriengeferitgte (commercial off-the-shelf) Produkte von **Dr.Web** bereits besitzen, ist es möglich, die vorhandene Schlüsseldatei für **Dr.Web antivirus** zu nutzen.

Um eine Lizenz zu erhalten oder zu registrieren, gehen Sie zu **Dr.Web - Lizenz** (s. Abbildungen 1a und 1b). Der Bereich **Dr.Web - Lizenz** wird beim ersten Start des Programms sowie beim Fehlen der Schlüsseldatei geöffnet. Außerdem können Sie diesen Bereich öffnen, indem Sie das App-menü auf dem Hauptbildschirm aufrufen (s. Abbildung 2). Wählen Sie den Punkt **Über das Programm** und danach drücken Sie die Taste **Lizenz verlängern**.

Dr.WEB
Das System ist nicht geschützt!
Um Dr.Web Antivirus nutzen zu können, müssen Sie sich registrieren und eine Lizenz- bzw. Demoschlüssel-Datei vom Doctor Web Server erhalten.
Demoversion
Kostenlose 14-Tage-Lizenz
Kaufen
Zum Online-Shop
Gültige Lizenz angeben
Nummer eingeben oder Datei auf der SD-Karte auswählen
Dr.WEB
Das System ist nicht geschützt!
Um Dr.Web Antivirus nutzen zu können, müssen Sie sich registrieren und eine Lizenz- bzw. Demoschlüssel-Datei vom Doctor Web Server erhalten.
Demoversion
Kostenlose 14-Tage-Lizenz
drweb.mikem@gmail.com
Kaufen/Herunterladen
Neue Lizenz kaufen/Eine zuvor gekaufte Lizenz herunterladen
Seriennummer eingeben
Geben Sie die Seriennummer an, die Sie beim Kauf erhalten haben

Abbildung 1a und 1b. Bildschirm Dr.Web - Lizenz

Lizenzschlüsseldatei

In der *Schlüsseldatei* sind u.a. folgende Informationen enthalten:

- Zeitraum, innerhalb dessen das Software-Produkt benutzt werden kann
- Liste der Komponenten, die der Nutzung zugänglich sind
- Sonstige Beschränkungen

Es gibt zwei Typen der Schlüsseldatei:

- *Lizenzschlüsseldatei*, die in Verbindung mit **Dr.Web antivirus** erworben wird und ermöglicht es, das Software-Produkt nicht nur zu nutzen, sondern auch den technischen Support in Anspruch zu nehmen. Die Parameter einer solchen Schlüsseldatei, durch die Benutzerrechte geregelt werden, werden gemäß der Lizenzvereinbarung konfiguriert. Darüber hinaus beinhaltet diese Datei auch Informationen zu Benutzer und Fachhändler.
- *Demoschlüsseldatei*, die dazu dient, um das Software-Produkt zu testen. Eine solche Schlüsseldatei sorgt für den vollen Funktionsumfang der Hauptkomponenten, hat aber eine beschränkte Gültigkeitsdauer.

Die Schlüsseldatei ist *gültig*, wenn folgende Bedingungen gleichzeitig erfüllt sind:

- Lizenz ist noch nicht abgelaufen
- Schlüsseldatei gilt für alle durch Programm benutzte Module
- Integrität des Schlüssels ist nicht beschädigt

Soll eine dieser Bedingungen nicht erfüllt werden, wird die Schlüsseldatei *ungültig*. Dabei werden die Schadprogramme durch Antivirus nicht mehr neutralisiert.

Durch die Bearbeitung wird die Schlüsseldatei ungültig! Es empfiehlt sich deshalb nicht, die Schlüsseldatei mit einem Texteditor zu öffnen, um deren zufällige Beschädigung zu vermeiden.

Schlüsseldatei erhalten

Demoschlüsseldatei erhalten

Wenn Sie das Programm installiert haben, um seine Funktionen zu testen, ist es möglich, eine kostenlose Lizenz für 14 Tage zu erhalten. Dafür wählen Sie die Option **Demo** im Bereich **Dr.Web - Lizenz** (s. Abbildungen 1a und 1b), geben Sie Ihre persönlichen Daten ein und drücken Sie die Taste **Schlüssel erhalten**:

- Haben Sie das Programm über Google Play installiert, wird die Schlüsseldatei für die E-Mail-Adresse registriert, die Sie bei der Anlegung Ihres Google-Kontos angegeben haben. Die Information dazu finden Sie unter **Demo** in dem Bereich **Dr.Web - Lizenz**. Wenn Sie mehrere Google-Konten besitzen, wird das erste davon ausgewählt. Sollten Sie kein Google-Konto besitzen, werden Sie gebeten, eine gültige E-Mail-Adresse zur Registrierung der Lizenz anzugeben.
- Wollen Sie die Demoschlüsseldatei für eine Anwendungsversion anfragen, die von der Website von **Doctor Web** heruntergeladen wurde, werden Sie gebeten, ein Formular mit Ihren persönlichen Daten auszufüllen. Füllen Sie bitte alle Felder des Formulars aus und klicken Sie auf **Schlüssel erhalten**.

In diesem Fall wird die Schlüsseldatei automatisch heruntergeladen und installiert. Nach Abschluss der Installation werden Informationen zu der erhaltenen Schlüsseldatei sowie ihrer Gültigkeitsdauer auf dem Bildschirm angezeigt.

Lizenz kaufen und Lizenzschlüsseldatei erhalten

Sie können die Lizenz für **Dr.Web antivirus**, je nachdem, wie die Anwendung installiert wurde, auf folgende Weise erwerben:

1. Wurde das Programm über Google Play installiert, wählen Sie im Bereich **Dr.Web - Lizenz** (s. Abbildungen 1a und 1b) die Option **Kaufen/Herunterladen** aus. Danach werden Sie gebeten, die E-Mail-Adresse zur Registrierung der Schlüsseldatei einzugeben. Dadurch werden Sie später Möglichkeit haben, die erworbene Schlüsseldatei für die Nutzung mit **Dr.Web antivirus** herunterzuladen, falls die Anwendung neu installiert bzw. auf einem anderen Gerät installiert wird.
   Im Dialogfenster **Lizenzkauf** können Sie eine von beiden Lizenztypen auswählen:
   - **1-Jahres-Lizenz**, **Lizenz für 2 Jahre** oder **Lizenz für 1 Jahr ohne Technischen Support**. Bei der Wahl einer dieser Varianten öffnet sich das Standardfenster für den Kauf der Anwendung. Kurz nach dem Abschluss des Zahlungsverfahrens wird die Lizenzschlüsseldatei auf Ihrem Gerät geladen. Nach Abschluss der Installation werden Informationen zu der Schlüsseldatei sowie ihrer Gültigkeitsdauer auf dem Bildschirm angezeigt. Wird das Herunterladen der Lizenzschlüsseldatei wegen möglicher technischer Störungen lange nicht gestartet, wenden Sie sich bitte an den Technischen Support von **Doctor Web**.
   - **Lizenz ohne zeitliche Begrenzung**. Bei der Wahl der Lizenz mit uneingeschränkter Gültigkeitsdauer werden Sie auf die Seite für Kauf und Installation von **Dr.Web Anti-virus Life license** bei Google Play weiter geleitet. Haben Sie bereits **Dr.Web antivirus** verwendet, werden Sie gebeten, es zu deinstallieren. Klicken Sie auf **OK**, um die Deinstallation zu bestätigen. Um die Anwendungseinstellungen für deren weitere Nutzung mit **Dr.Web antivirus Life license** aufzubewahren, können Sie die Einstellungen vor Deinstallation exportieren.

Ist die **Dr.Web Anti-Theft**-Funktion auf Ihrem Gerät aktiviert, müssen Sie, bevor Sie **Dr.Web antivirus** deinstallieren, die Markierung des Kontrollkästchens **Dr.Web Antivirus** auf der Registerkarte **Einstellungen - Standort und Sicherheit** im Abschnitt **Geräte-Administratoren** in den Einstellungen des Telefons (Einstellungen können bei unterschiedlichen Telefonmodellen und Versionen des Betriebssystems voneinander abweichen) aufheben. Das Gerät wird daraufhin durch **Dr.Web Anti-Theft** gesperrt. Geben Sie das für **Dr.Wen Anti-Theft** angelegte Passwort ein, um mit der Deinstallation der Anwendung fortzusetzen.

Bei der Installation einer Lizenzversion von **Dr.Web antivirus Life license** wird die Lizenzschlüsseldatei automatisch heruntergeladen und installiert.

2. Wenn Sie das Programm auf der Website von **Doctor Web** heruntergeladen und installiert haben, können Sie die Lizenz für **Dr.Web antivirus** im Online-Shop von **Doctor Web** erwerben. Wählen Sie dazu die Option **Kaufen** im Bereich **Dr.Web - Lizenz** aus oder öffnen Sie in Ihrem Browser die Seite http://estore.drweb-av.de/mobile/. Wählen Sie die Gültigkeitsdauer der Lizenz und die Anzahl der geschützten Geräte aus und tippen Sie auf **Kaufen**. In diesem Fall wird die Seriennummer bzw. die Lizenzschlüsseldatei an die bei der Bestellung angegebene E-Mail-Adresse zugesendet. Des Weiteren können Sie die Seriennummer als eine SMS-Nachricht an die von Ihnen bei der Registrierung angegebene Rufnummer erhalten. Danach müssen Sie die Seriennummer registrieren bzw. die Schlüsseldatei auf mobiles Endgerät kopieren.

Schlüsseldatei verwenden

Wenn Sie eine Schlüsseldatei für **Dr.Web antivirus** bereits besitzen, bzw. eine Lizenz für **Dr.Web Security Space**, **Dr.Web Desktop Security Suite** oder beliebige handelsübliche, seriengeferitgte (commercial off-the-shelf) Produkte von **Dr.Web** bereits besitzen, können Sie die vorhandene Lizenz je nachdem, wie **Dr.Web antivirus** auf Ihrem Gerät installiert wurde, auf folgende Weise registrieren und nutzen:

1. Haben Sie **Dr.Web antivirus** über Google Play installiert und die Demoschlüsseldatei bzw. die Lizenzschlüsseldatei bereits erhalten, wählen Sie im Bereich **Dr.Web - Lizenz** (s. Abbildungen 1a und 1b) die Option **Kaufen/Herunterladen** aus. Geben Sie bei Bedarf die E-Mail-Adresse ein, die Sie zum Erhalten/Registrieren der Schlüsseldatei bereits verwendet haben. Die Lizenzdatei, die für die angegebene E-Mail-Adresse registriert wurde, wird automatisch von dem Server heruntergeladen und installiert. Sollten Sie eine Seriennummer besitzen, gebein Sie diese ein, um die Schlüsseldatei auf Ihrem Gerät über eine Interneverbindung herunterzuladen.
2. Wurde **Dr.Web antivirus** von der Website von **Doctor Web** heruntergeladen und installiert, können Sie die vorhandene Schlüsseldatei in einen speziellen Ordner auf einer SD-Karte kopieren bzw. die Seriennummer zum Erhalten der Lizenzschlüsseldatei über E-Mail oder zum Herunterladen auf Ihrem mobilen Gerät über eine Internetverbindung registrieren.

Die Schlüsseldatei von **Dr.Web Security Space** bzw. **Dr.Web Security Space Pro** kann für **Dr.Web antivirus** benutzt werden, wenn sie DrWebGUI unterstützt.

Um die Möglichkeit, die Schlüsseldatei zu nutzen, zu überprüfen, gehen Sie wie folgt vor:

1. Öffnen Sie die Schlüsseldatei mit einem Texteditor (z. B. mit Notepad).
2. Überprüfen Sie, ob die DrWebGUI-Komponente in der Liste mit Werten für den Parameter Applications in der Gruppe [Key] vorhanden ist: ist diese Komponente in der Liste vorhanden, kann die Schlüsseldatei für **Dr.Web antivirus** benutzt werden.

Die Schlüsseldatei hat ein Format, das vor Bearbeitung geschützt ist. Durch die Bearbeitung wird die Datei ungültig. Um die Beschädigung der Schlüsseldatei zu vermeiden, empfiehlt es sich nicht, sie beim Beenden des Texteditors zu speichern.

Schlüsseldatei auf ein mobiles Endgerät kopieren

1. Kopieren Sie die Schlüsseldatei in den Ordner **Android/data/com.drweb/files**, der sich auf der SD-Karte befindet.
2. Im Bereich **Dr.Web - Lizenz** (s. Abbildungen 1a und 1b) wählen Sie den Punkt **Gültige Lizenz angeben**.
3. Wählen Sie den Punkt **Aus der Datei laden**. Im Infofenster **Schlüssel aus der Datei** drücken Sie die **OK**-Taste.
4. Die Schlüsseldatei wird installiert und ist somit zur Nutzung bereit. Es öffnet sich ein Fenster mit Informationen zu Gültigkeitsdauer der Lizenz. Drücken Sie die **OK**-Taste.

Lizenzschlüsseldatei bei der Registrierung der Seriennummer erhalten

Sie können die Lizenzschlüsseldatei per E-Mail nach der Registrierung des Software-Produktes auf der offiziellen Website von **Doctor Web** erhalten. Dafür gehen Sie wie folgt vor:

1. Öffnen Sie die Website, deren Adresse in der mit dem Produkt gelieferten Registrierkarte angegeben ist.
2. Geben Sie die Seriennummer für Registrierung ein (die Nummer finden Sie in der Registrierkarte).
3. Füllen Sie das Formular mit Angaben zum Käufer aus.
4. Die Schlüsseldatei wird als ein ZIP-Archiv mit der .key-Datei an die von Ihnen angegebene E-Mail-Adresse zugesendet.

5. Entpacken Sie die Datei auf den Computer, von dem sie auf das mobile Endgerät kopiert werden kann.

Darüber hinaus können Sie die Lizenzschlüsseldatei direkt auf das mobile Endgerät über Internet herunterladen. Dafür gehen Sie wie folgt vor:

1. Im Bereich **Dr.Web - Lizenz** (s. Abbildungen 1a und 1b) wählen Sie die Variante **Gültige Lizenz angeben**.
2. Wählen Sie den Punkt **Seriennummer eingeben**.

Die Seriennummer, die zur Aktivierung des Testzeitraums für eines der **Dr.Web** Produkte für Workstations erhalten wurde, kann nicht für die aus Google Play installierte Version von **Dr.Web antivirus** verwendet werden. In diesem Fall müssen Sie zuerst den Testzeitraum für das **Dr.Web** Produkt auf dem PC aktivieren. Dabei erhalten Sie die entsprechende Lizenzschlüsseldatei. Danach können Sie diese auf das mobile Endgerät kopieren. Die Anleitungen zur Nutzung der erhaltenen Lizenzschlüsseldatei erhalten Sie per E-Mail bei Aktivierung des Testzeitraums.

3. Geben Sie die Seriennummer ein und drücken Sie die Taste **Schlüssel erhalten**.
4. Wird diese Seriennummer zum ersten Mal registriert, öffnet sich ein Bereich zur Eingabe der persönlichen Daten, die beim Erhalten der Schlüsseldatei benötigt werden. Füllen Sie alle Felder aus und drücken Sie die Taste **Schlüssel erhalten**.
5. Es wird ein Verfahren zum Herunterladen und zur Installation der Schlüsseldatei gestartet. Das entsprechende Protokoll wird in einem separaten Infofenster angezeigt:
   - Wenn die Schlüsseldatei erfolgreich erhalten ist, drücken Sie die **OK**-Taste.
   - Sind Fehler beim Erhalten der Schlüsseldatei aufgetreten, wird eine Beschreibung des entstandenen Problems angezeigt.

Lizenz verlängern

In manchen Fällen, z. B. bei Lizenzablauf, kann es erforderlich sein, die bereits vorhandene und im System registrierte Lizenzschlüsseldatei zu ersetzen. **Dr.Web antivirus** unterstützt die "on the fly"-Aktualisierung der Schlüsseldatei. Dabei brauchen Sie nicht, die Schlüsseldatei neu zu installieren bzw. ihre Nutzung zu unterbrechen.

Informationen zur Lizenz

Um Informationen zur genutzten Lizenz einzusehen:

1. Auf dem Hauptbildschirm des Programms (s. Abbildung 2) rufen Sie das App-Menü auf und wählen Sie den Punkt **Über das Programm**.
2. Im Bereich **Dr.Web - Über das Programm** können Sie folgende Informationen zur Lizenz einsehen:
   - Name des Lizenzinhabers
   - Registrierungs- sowie Ablaufdatum der Lizenz

Benachrichtigungen konfigurieren

Sie können die Benachrichtigungen über eine bald ablaufende Lizenz aktivieren/deaktivieren. Dazu navigieren Sie zu **Benachrichtigungen** in dem Bereich **Lizenz** auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6).

Lizenz aktualisieren

Für die Aktualisierung der Lizenz müssen Sie eine neue Schlüsseldatei erhalten oder registrieren.

Sie können auch eine neue Lizenz erwerben bzw. die aktuelle Lizenz in Ihrem persönlichen Berieich auf der offiziellen Website von **Doctor Web** verlängern. Folgen Sie bitte dem Link unter **Mein D.Web** auf dem Bildschirm **Dr.Web - Über das Programm**, um die Website im Browserfenster zu öffnen.

Kapitel 3. Installation und Deinstallation

Dr.Web antivirus kann direkt über den Google Play Store erworben und installiert werden. Sie können auch die Installationsdatei für **drweb-901-android.apk** auf Ihr mobiles Gerät kopieren und dort ausführen. Darüber hinaus ist es auch möglich, ein Programm zum Synchronisieren mit PC für Installation der Anwendung zu nutzen.

Das Programm kann über Google Play bzw. mit normalen Betriebssystemmitteln des mobilen Endgeräts gelöscht werden.

Systemanforderungen

Zur Installation und Nutzung von **Dr.Web antivirus** wird es benötigt, dass das mobile Gerät unter einem Android-Betriebssystem der Version 2.1/2.2/2.3/3.0/3.1/3.2/4.0/4.1/4.2/4.3/4.4 läuft.

Außerdem benötigen Sie eine Internetverbindung, um Updates für Virendatenbanken herunterzuladen. Wenn Sie einen Tablet-PC verwenden, muss es die Möglichkeit bestehen, eine SIM-Karte einzulegen und zu nutzen, damit Filtern der Nachrichten und **Dr.Web Anti-Theft** funktionieren. Darüber hinaus ist die Firewall nur auf den Geräten mit Android 4.0 oder höher verfügbar.

Bitte beachten Sie, dass kein korrekter Betrieb von **Dr.Web antivirus** bei Geräten mit der durch Benutzer veränderten Firmware bzw. mit Root-Zugriff (sogenannte gerootete Geräte) garantiert werden kann! Des Weiteren wird kein technischer Support für solche Geräte geleistet.

Programm installieren

Dr.Web antivirus kann über Google Play sowie durch Ausführen der Installationsdatei auf dem mobilen Gerät bzw. mit Hilfe eines Programms zum Synchronisieren mit PC installiert werden.

Anwendung über Google Play installieren

1. Öffnen Sie Google Play und finden Sie **Dr.Web antivirus** in der Anwendungsliste. Drücken Sie die Taste **Installieren** bzw. **Kaufen** je nach der Version der Anwendung.

   Wenn **Dr.Web antivirus** im Google Play nicht zu finden ist, heisst es, dass mobiles Endgerät minimale Systemanforderungen nicht erfüllt.

2. Wenn Sie die Anwendungsversion mit der uneingeschränkten Lizenz installieren (**Dr.Web Anti-virus Life license**), es öffnet sich der Bildschirm mit Zahlungsoptionen.
3. Nachdem Zahlung geleistet wird, öffnet sich Information zu Zugriffsrechten, die durch Anwendung benötigt werden. Das Programm erfordert Zugriff auf folgende Daten:
   - Bei der Installation der Antivirensoftware **Dr.Web antivirus** für einen kostenlosen Testzeitraum (14 Tage) wird der Zugriff auf die In-App-Kauf-Funktion für den Lizenzerwerb benötigt, nachdem der Testzeitraum abgelaufen ist;
   - zum Registrieren der Anwendung und Aktivieren der Lizenz wird ein Internetzugriff sowie Zugriff auf die Liste der Google-Konten auf dem Gerät benötigt;
   - damit der Datei-Wächter **SpIDer Guard** und der Scanner funktionieren, wird Zugriff auf den Gerät-Speicher, die Daten der Anwendungen und die SD-Karte sowie eine Möglichkeit zum Lesen und Schreiben von Daten benötigt;

- zum Filtern von Anrufen und SMS-Nachrichten benötigt man Zugriff auf Sende- und Empfangsfunktionen sowie eine Möglichkeit, die Kontaktliste und den Anruf- und SMS-Nachrichtenverlauf zu lesen, den Signalmodus zu ändern (um den Ton auszuschalten, wenn der Anruf gesperrt wird);
- damit **Dr.Web Anti-Theft** funktioniert, wird Zugriff auf SMS-Sendefunktionen (um Nachrichten von **Dr.Web Anti-Theft** über den SIM-Kartenwechsel sowie Antworten auf gesendete Befehle zu senden), Ortungsfunktionen, Funktionen zur GPS- und Wi-Fi-Verwaltung sowie eine Möglichkeit, alle persönlichen Daten auf dem Gerät zu löschen (wenn ein entsprechender Befehl empfangen wird), benötigt;
- zur Funktion des **Cloud Checker** URL-Filters wird Zugriff auf Verlauf und Lesezeichen der unterstützten Browser benötigt;
- zur Aktualisierung von Virendatenbanken wird ein Internetzugriff sowie Zugriff auf die Netzwerkeinstellungen des Geräts benötigt.

Drücken Sie die **OK**-Taste.

4. Die Anwendung wird automatisch installiert.

Um die Anwendung ohne Verwendung von Google Play zu installieren, müssen Sie eine solche Installationsart erlauben. Dafür öffnen Sie den Bereich **Einstellungen** -> **Apps** und setzen Sie ein Häkchen bei **Unbekannte Quellen**. Die Installationsdatei **Dr.Web antivirus** kann von der Website von **Doctor Web** unter http://download.drweb-av.de/android heruntergeladen werden.

Installationsdatei drweb-901-android.apk direkt auf dem mobilen Gerät ausführen

1. Kopieren Sie die Installationsdatei **drweb-901-android.apk** auf Speicherkarte.

Zur Suche und Ausführung der Datei auf dem mobilen Endgerät wird ein Datei-Browser benötigt.

2. Verwenden Sie den Datei-Browser, um die Installationsdatei zu finden und auszuführen.
3. Die Anwendung wird automatisch installiert.

Installation mit Hilfe des Programms zum Synchronisieren des mobilen Endgeräts mit PC (z.B. HTC Sync™ u. a.)

1. Synchronisieren Sie Ihr mobiles Gerät mit PC.
2. Starten Sie den Anwendungsinstallations-Assistenten, der zum Umfang der Synchronisationssoftware gehört.
3. Geben Sie den Pfad der Installationsdatei **drweb-901-android.apk** auf dem Computer an und folgen Sie den Anweisungen des Installationsassistenten.
4. Die Anwendung wird auf das mobile Gerät übertragen. Somit können Sie die Informationen dazu einsehen und die Installation akzeptieren.
5. Beenden Sie den Installationsassistenten der Synchronisationssoftware.

Dr.Web antivirus ist installiert und zur Nutzung bereit. Wenn die Anwendung ohne Verwendung von Google Play installiert wird, müssen Sie die Lizenz registrieren, um diese Anwendung nutzen zu können. Wenn Sie keine gültige Schlüsseldatei haben, nutzen Sie das Verfahren zum Erhalten der Schlüsseldatei.

Standardmäßig wird die Anwendung in den internen Speicher des mobilen Geräts installiert. Damit die Anwendung und im besonderen die Funktion **Dr.Web Anti-Theft** richtig funktionieren kann, wird es nicht empfohlen, die installierte Anwendung auf externe Datenträger zu übertragen.

Programm deinstallieren und aktualisieren

Sie können die Programmversion über Google Play aktualisieren bzw. es von Ihrem mobilen Gerät löschen. Außerdem ist es möglich, das Programm mit Betriebssystemmitteln ohne Internetverbindung zu entfernen.

Wenn **Dr.Web Anti-Theft** auf Ihrem Gerät aktiviert ist, muss man das Häkchen bei **Dr.Web Antivirus** unter **Einstellungen** - **Standort und Sicherheit** - **Geräte-Administratoren** vor Löschen der Anwendung abwählen (Die Bezeichnungen für die Einstellungsoptionen können sich je nach Modell des Telefons bzw. Version des Betriebssystems unterscheiden).

Programm über Google Play deinstallieren und aktualisieren

1. Öffnen Sie den Google Play Store und wählen Sie den Punkt **Meine Downloads** oder **Meine Apps** (je nach verwendeter Version des Betriebssystems).
2. In der Liste der auf dem mobilen Gerät installierten Anwendungen drücken Sie das Icon von **Dr.Web antivirus**.

   Wenn **Dr.Web antivirus** ohne Verwendung von Google Play installiert wurde, kann die Anwendung im Bereich **Meine Downloads** fehlen. In diesem Fall können Sie das Programm mit Betriebssystemmitteln löschen.

3. Auf dem Bildschirm mit Informationen zu Anwendung drücken Sie die Taste **Aktualisieren**, um neue Version zu installieren, bzw. die Taste **Deinstallieren**, um das Programm zu löschen.
4. Bestätigen Sie die Aktualisierung/Deinstallation der Anwendung:
   - Bei der Aktualisierung fallen weitere Schritte mit den im Abschnitt Programm installieren beschriebenen Schritten zusammen.
   - Wenn das Programm gelöscht wird, geben Sie die Ursache für Deinstallation des Programms an und drücken Sie die **OK**-Taste. Das Programm wird von Ihrem mobilen Gerät deinstalliert.

Programm ohne Internetverbindung deinstallieren

1. Öffnen Sie den Bereich **Einstellungen** -> **Apps** -> **Apps verwalten**.
2. In der Liste der auf dem mobilen Gerät installierten Anwendungen drücken Sie das Icon von **Dr.Web antivirus**.
3. Auf dem Bildschirm mit Informationen zur Anwendung drücken Sie die Taste **Deinstallieren**. Das Programm wird von Ihrem mobilen Gerät gelöscht.
4. Nachdem die Deinstallation beendet wird, drücken Sie die **OK**-Taste, um zur Liste der installierten Anwendungen zurück zu wechseln.

Die Quarantäne und das gespeicherte Ereignislog werden standardmäßig nicht gelöscht. Gegebenenfalls können Sie diese aus dem Ordner Android/data/com.drweb/files auf der SD-Karte manuell löschen.

Verfügbarkeit der neuen Programmversion prüfen

Wenn Sie **Dr.Web antivirus** von der Website von **Doctor Web** heruntergeladen und installiert haben, können Sie die Einstellungen so konfigurieren, dass die Verfügbarkeit der neuen Programmversion bei jeder Aktualisierung der Virendatenbanken des Programms geprüft wird. Markieren Sie dazu das Kontrollkästchen **Neue Version der Anwendung** im Abschnitt für die Einstellung der Aktualisierungen des Programms. Erscheint eine neue Anwendungsversion, werden Sie darüber standardmäßig informiert und können die neue Version schnell herunterladen und installieren.

Kapitel 4. Mit der Arbeit beginnen

Dieser Abschnitt beschreibt das Verfahren zum Starten und Beenden von **Dr.Web antivirus** sowie die Benutzeroberfläche der Anwendung.

Antivirusprogramm starten und beenden

Programm starten

Um **Dr.Web antivirus** zu starten, öffnen Sie den Bereich **Alle** und drücken Sie das Icon von **Dr.Web antivirus** . Beim ersten Start des Programms öffnet sich die Lizenzvereinbarung, die Sie für weitere Arbeit zu akzeptieren brauchen. In diesem Fenster können Sie sich auch mit Informationen über das Programm zur Verbesserung der Software-Qualität vertraut machen sowie Ihre Teilnahme daran akzeptieren, indem Sie sich mit einem automatischen Versand nicht-personenbezogener Daten zu entdeckten Bedrohungen und besuchten Websites an Server von **Doctor Web** und Google einverstanden erklären. Sie können zu jeder Zeit auf Versand dieser Statistik in den Einstellungen der Anwendung verzichten. Dafür wählen Sie das Häkchen bei **Statistik senden** im Bereich **Allgemein** ab.

Programm beenden

Um die Anwendung zu beenden, drücken Sie die **Home**-Taste .

Zum wiederholten Start der Anwendung können Sie das Icon von **Dr.Web antivirus** im Bereich für zuletzt gestartete Anwendungen tippen.

Beim ersten Starten öffnet sich **Dr.Web antivirus** auf dem Hauptbildschirm. Beim wiederholten Starten öffnet sich das Programm in dem Bereich, der zuletzt aktiv war, wenn das Programm beendet wurde.

Oberfläche

Der Hauptbildschirm von **Dr.Web antivirus** (s. Abbildung 2) beinhaltet Informationen zum aktuellen Stand des Systems. Darüber hinaus lassen sich folgende Funktionen des Programms darüber konfigurieren:

- **SpIDer Guard** – damit lässt sich der permanente Virenschutz aktivieren/deaktivieren
- **Anruf- und Nachrichtenfilter** – ermöglicht es, den Filterungsmodus zu wählen sowie die Listen der gesperrten Anrufe und Nachrichten einzusehen

Auf den Tablet-PCs ohne SIM-Karte ist der Anruf- und Nachrichtenfilter nicht verfügbar. Demgemäß gibt es keinen solchen Bereich auf dem Hauptbildschirm der Anwendung.

- **Scanner** – überprüft das System auf Anforderung des Benutzers (3 Prüfungsarten stehen zur Verfügung: schnell, vollständig und benutzerdefiniert)
- **Update** – beinhaltet Informationen zum Datum des letzten Updates und ermöglicht es, die Aktualisierung des Programms bei Bedarf zu starten
- **Anti-Theft** – ermöglicht es, die Funktionen von **Dr.Web Anti-Theft** zu konfigurieren
- **Cloud Checker** – damit lässt sich der URL-Filter zur Einschränkung des Benutzerzugriffs auf die Webinhalte konfigurieren
- **Firewall** – ermöglicht es, die Überwachung der Internetverbindungen und die Datenübertragung im Netzwerk zu konfigurieren;

- **Security Auditor** – ermöglicht es, das System zu analysieren und erkannte Sicherheitsprobleme und -lücken zu beseitigen

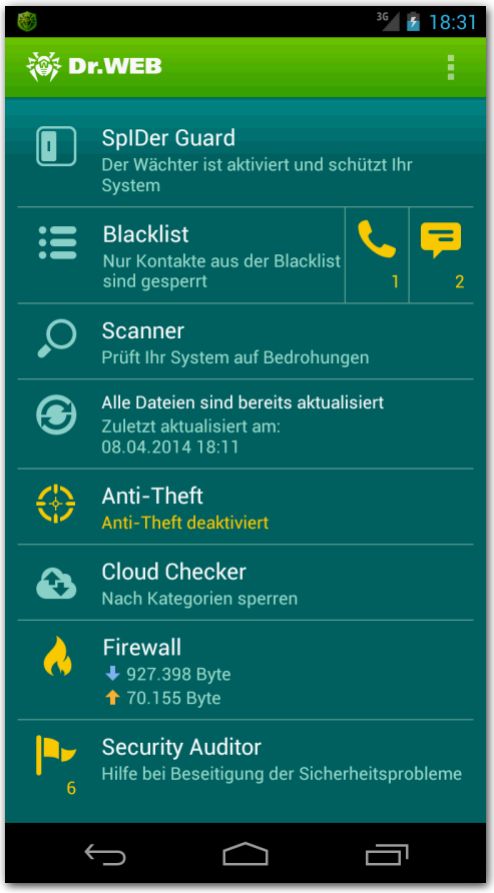


Abbildung 2. Hauptbildschirm des Programms

Auf Anwendungsmenü zugreifen und zwischen den Bildschirmen navigieren

Auf den Anwendungsbildschirmen mit zusätzlichen Optionen wird das Menü mit einer Taste oben in der rechten Bildschirmecke aufgerufen. Um zurück zum vorherigen Bildschirm zu wechseln, tippen Sie auf das Anwendungssymbol oben links.

Mit dem Hauptbildschirm-Menü können Sie die App-Einstellungen öffnen, auf die Quarantäne und deren Statistiken zugreifen sowie Informationen über das Programm einsehen. In dem Bereich **Dr.Web - Über das Programm** sind Informationen zu Anwendungsversion und Anzahl der Signaturen in den **Dr.Web Virendatenbanken** sowie zu Inhaber und Aktivierungs- und Ablaufdaten der Lizenz untergebracht. In diesem Bereich finden Sie auch Links zur offiziellen Website von **Doctor Web**, zu Ihrem persönlichen Bereich auf der offiziellen Website sowie zu unseren Profilen in sozialen Netzwerken Twitter, Facebook, Instagram und Youtube.

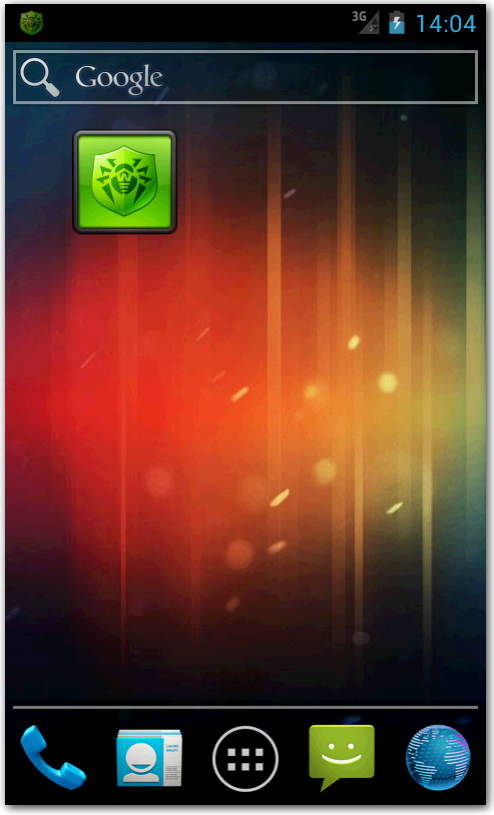
Widgets

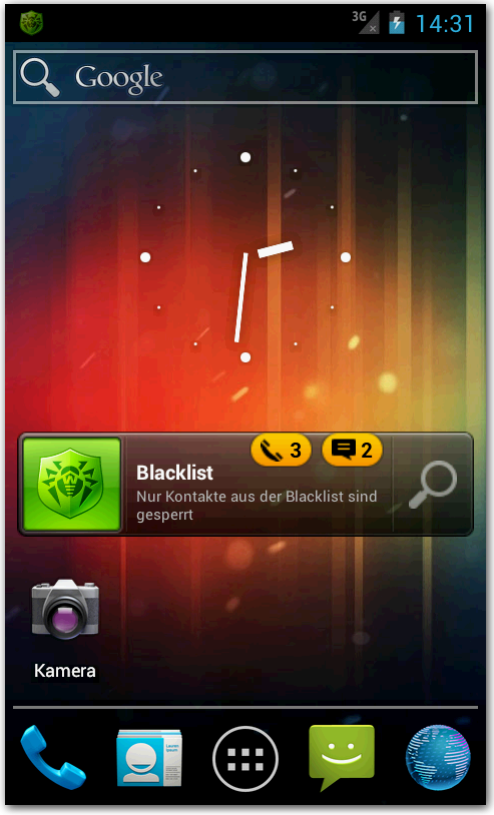
Für eine bequeme Nutzung von **Dr.Web antivirus** können Sie spezielle Widgets auf den **Startbildschirm** Ihres Telefons bringen. Mit diesen Widgets lassen sich die Hauptfunktionen des Programms verwalten.

Widget hinzufügen

1. Widgets werden mit Hilfe von Standardverfahren Ihres Betriebssystems hinzugefügt. Öffnen Sie die Liste von Widgets, die auf Ihrem Gerät hinzugefügt werden können.

2. In der Liste der verfügbaren Widgets wählen Sie eines der Widgets von **Dr.Web antivirus**:
   - **Dr.Web 1x1 (klein)** – zeigt den aktuellen Schutzstatus und ermöglicht die Aktivierung/Deaktivierung von **SpIDer Guard** (s. Abbildung 3).
   - **Dr.Web 4x1 (mittelgroß)** – zeigt den aktuellen Schutzstatus, das aktuelle Filterprofil, die Anzahl der gesperrten Anrufe und Nachrichten sowie ermöglicht die Aktivierung/Deaktivierung von **SpIDer Guard**, den Übergang zum Scan-Bildschirm (s. Abbildung 4).





Abbildungen 3 und 4. Dr.Web Widgets

Benachrichtigungen

Um auf Grundfunktionen von **Dr.Web antivirus** schnell zuzugreifen, können Sie die spezielle Benachrichtigungsleiste oben auf dem Bildschirm nutzen (s. Abbildung 5). Um diese Leiste zu aktivieren/deaktivieren, navigieren Sie zu **Benachrichtigungsleiste** im Bereich **Allgemein** auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6).

Abbildung 5. Benachrichtigungsleiste

Die Benachrichtigungsleiste bietet folgende Möglichkeiten:

- zum Bildschirm von **Dr.Web antivirus** wechseln. Tippen Sie dazu auf das **Dr.Web**-Symbol.
- schnelles, vollständiges bzw. benutzerdefiniertes Scannen starten. Wählen Sie dazu die Option **Scanner** und entsprechenden Scanvorgang aus.
- Filterprofil für Anrufe und Nachrichten anhand der Option **Profil** wählen.

Wenn Ihr Gerät keine SIM-Karten unterstützt, wird die Option **Downloads** anstatt der Option **Profil** in der Benachrichtigungsleiste angezeigt. Diese Option ermöglicht es, dass die auf das Gerät heruntergeladene Objekte durchsucht werden.

- zum Einstellungsbildschirm des URL-Filters anhand der Option **Cloud Checker** wechseln.

Sollten Bedrohungen erkannt werden, ändern sich die entsprechenden Symbole in der Benachrichtigungsleiste:

- – wenn die Bedrohungen durch den Scanner erkannt wurden;
- – wenn die Bedrohungen durch den Datei-Wächter **SpIDer Guard** erkannt wurden.

Mein Dr.Web

Nutzen Sie den Online-Service **Mein Dr.Web**, um Ihren persönlichen Bereich auf der Website von **Doctor Web** zu besuchen. Auf dieser Internetseite finden Sie Informationen zu Ihrer Lizenz (Gültigkeitsdauer, Seriennummer). Weiterhin können Sie die aktuelle Lizenz verlängern, das Datum und die Uhrzeit des letzten Updates sowie die Anzahl der Signaturen in den Virendatenbanken einsehen,

Nachrichten und Sonderangebote erhalten, eine Frage an technischen Support stellen und a.m.

Um diese Webseite zu öffnen, rufen Sie das Anwendungsmenü auf dem Hauptbildschirm auf (s. Abbildung 2) und wählen Sie **Über das Programm**. Tippen Sie auf **Mein Dr.Web** auf dem Bildschirm **Dr.Web - Über das Programm**.

Kapitel 5. Programmfunktionen und -einstellungen

Dieser Abschnitt beschreibt die grundsätzlichen Möglichkeiten von **Dr.Web antivirus**, mit denen sich die Virenprüfung, der Anruf- und Nachrichtenfilter, die Funktion von **Dr.Web Anti-Theft**, der URL-Filter konfigurieren sowie der Schutz des mobilen Geräts auf solche Weise einrichten lässt.

Die Funktion der Hauptkomponenten von **Dr.Web antivirus** erfolgt im Bereich **Dr.Web - Einstellungen** (s. Abbildung 6). Um zum Bildschirm mit Anwendungseinstellungen zu wechseln, müssen Sie auf dem Haupt-Bildschirm des Programms das Anwendungsmenü aufrufen, dann den Punkt **Einstellungen** wählen.

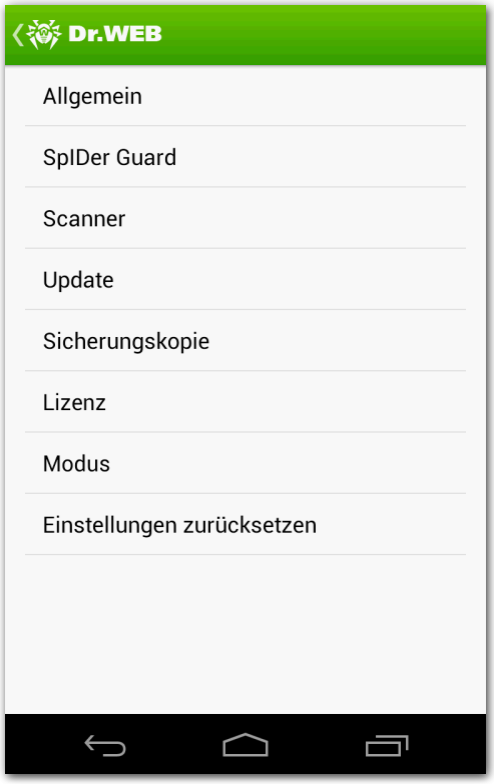


Abbildung 6. Bildschirm Dr.Web - Einstellungen

Einstellungen zurücksetzen

Sie können jeden Augenblick die benutzerdefinierten Einstellungen der Anwendung zurücksetzen und die Standard-Einstellungen wiederherstellen. Dafür gehen Sie wie folgt vor:

1. Auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6) im Bereich **Einstellungen zurücksetzen** wählen Sie den Punkt **Standardeinstellungen wiederherstellen**.
2. Bestätigen Sie die Wiederherstellung von Default-Einstellungen.

Einstellungen importieren und exportieren

Es ist möglich, alle aktuellen Einstellungen der Anwendung in einer Datei auf der SD-Karte zu speichern. Gegebenenfalls (z.B. wenn **Dr.Web antivirus** neu installiert bzw. auf einem anderen Gerät benutzt wird) können Sie später diese Einstellungen aus der Datei herunterladen.

1. Um aktuelle Konfiguration zu speichern, wählen Sie den Punkt **Exportieren von Daten** im Bereich **Sicherungskopie** auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6). Im geöffneten Fenster geben Sie das Passwort für die Konfigurationsdatei ein und drücken Sie auf **OK**. Alle Programmeinstellungen und -Daten werden in der Datei Android/data/com.drweb/files/DrWebPro.bkp auf der SD-Karte gespeichert.

2. Um die Einstellungen aus der Datei zu laden, wählen Sie den Punkt **Importieren von Daten** im Bereich **Sicherungskopie** auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6). Bestätigen Sie das Herunterladen von Parametern aus der Datei und geben Sie das Passwort der Konfigurationsdatei ein. Alle aktuellen Einstellungen werden gelöscht und durch die aus der Datei heruntergeladenen Einstellungen ersetzt.

Virenschutz

Die Hauptfunktion, die durch **Dr.Web antivirus** realisiert wird, ist eine permanente Überprüfung des Dateisystems in der Echtzeit. Darüber hinaus scannt **Dr.Web antivirus** das System auf Anforderung des Benutzers. Wenn Sicherheitsbedrohungen entdeckt werden, werden die durch Benutzer ausgewählten Aktionen dafür verwendet.

Permanenter Virenschutz

Die permanente Echtzeit-Prüfung des Dateisystems erfolgt mit Hilfe des **SpIDer Guard** *Dateiwächters*. Er überprüft alle Dateien, beim Versuch sie im Speicher des mobilen Geräts zu speichern. Somit wird das System vor Sicherheitsbedrohungen geschützt.

Permanenten Schutz aktivieren

Beim ersten Starten von **Dr.Web antivirus** wird der permanente Schutz automatisch nach Akzeptieren der Lizenzvereinbarung aktiviert. Um den Schutz zu deaktivieren bzw. erneut zu aktivieren, tippen Sie auf den Bereich **SpIDer Guard** auf dem Haupt- Bildschirm des Programms.

Beim Aktivieren beginnt der Wächter, Ihr System zu schützen. Er funktioniert weiter unabhängig davon, ob die Anwendung gestartet ist oder nicht. Wenn Sicherheitsbedrohungen entdeckt werden, erscheint das Warnzeichen in der Statusleiste im oberen Bildschirmbereich sowie ein Fenster mit Informationen zu entdeckten Bedrohungen. Im Benachrichtigungen-Bereich können Sie die Informationen zu Anzahl entdeckter Bedrohungen einsehen und die Liste der Bedrohungen öffnen, um Aktionen zu deren Neutralisierung auszuführen.

Der Dateiwächter wird gestoppt, wenn der Speicher Ihres Geräts im integrierten Task-Manager komplett geleert wird. In diesem Fall müssen Sie **Dr.Web antivirus** wiederholt öffnen, um ständigen Virenschutz wiederherzustellen.

Einstellungen des Dateiwächters

Für den Zugriff auf die Einstellungen von **Dr.Web antivirus** auf dem Haupt- Bildschirm des Programms rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen**. Um den Dateiwächter zu konfigurieren, gehen Sie auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6) wie folgt vor:

- Um die Prüfung von Dateien in Archiven zu aktivieren, setzen Sie ein Häkchen bei **Dateien in Archiven** im Bereich **SpIDer Guard**.

Standardmäßig ist die Archivprüfung deaktiviert. Durch die Aktivierung der Archivprüfung kann die Operationsgeschwindigkeit des Betriebssystems beschränkt und die Batterielaufzeit reduziert werden. Dabei beeinflusst die Deaktivierung von Archivprüfung den Schutzstatus nicht, da die Installationsdateien für Android-Betriebssystem (.apk) durch den Dateiwächter jedenfalls überprüft werden, unabhängig davon, welcher Wert für diesen Parameter festgelegt wurde.

- Um die Prüfung von SD-Karte bei jedem Anschließen an das mobile Gerät zu aktivieren, setzen Sie ein Häkchen bei **SD-Karte anschließen** im Bereich **SpIDer Guard**.
- um die Überprüfung des Systems auf Adware und PUAs (darunter auch Dialer und Scherzprogramme) zu aktivieren/deaktivieren, wählen Sie den Punkt **Optionen** im Bereich **SpIDer Guard** und setzen/ wählen Sie Häkchen bei **Adware** und **Riskware** ab;
- Um die SD-Karte auf Windows-Autostart-Dateien zu überprüfen, setzen Sie ein Häkchen bei **Autorun-Dateien** im Bereich **Allgemein**. Diese Einstellung wird auch beim Scannen auf

Anforderung des Benutzers verwendet.

- Um die Anzeige des Programmsymbols in der Statusleiste bei der Aktivierung des Dateiwächters zu aktivieren, setzen Sie ein Häkchen bei **Dr.Web Icon** im Bereich **Allgemein**.

Statistik

Das Programm registriert die Ereignisse, die mit dem Betrieb des Dateiwächters (Aktivierung/ Deaktivierung, Ergebnisse der Prüfung von SD-Karte sowie von den zu installierenden Anwendungen, Entdeckung von Sicherheitsbedrohungen) verbunden sind. Die Aktionen des Programms und insbesondere des Dateiwächters werden im Bereich **Aktionen** im Tab **Statistik** nach Datum sortiert angezeigt.

Überprüfung auf Anforderung des Benutzers

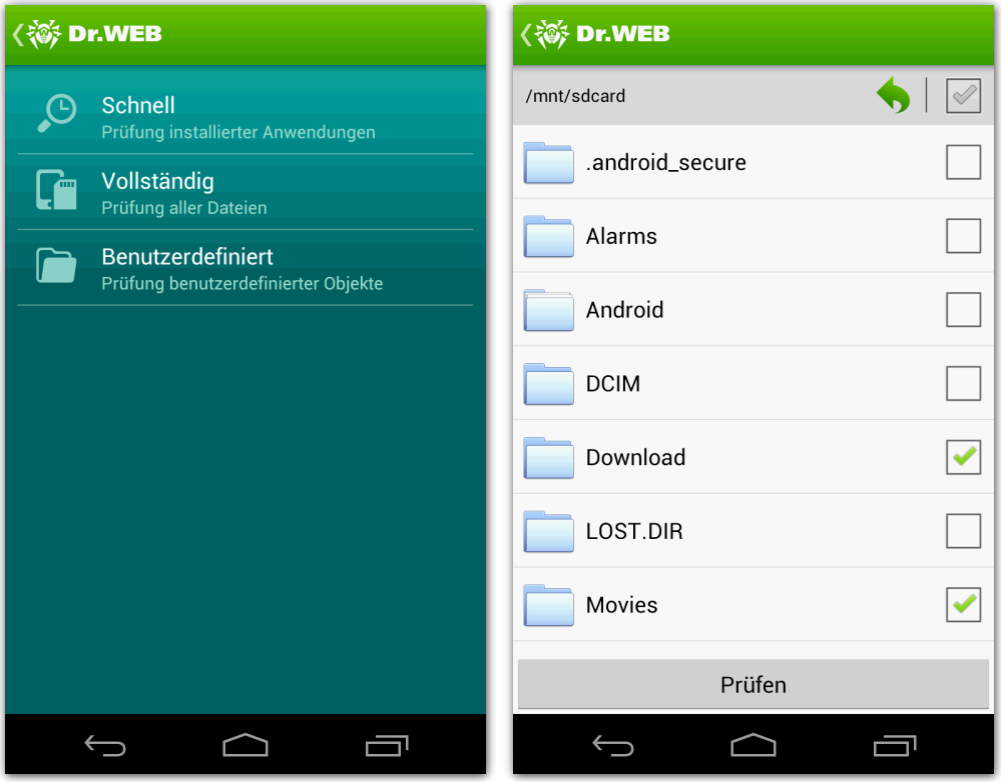
Das System wird auf Anforderung des Benutzers mit Hilfe einer speziellen Komponente –- eines *Scanners* –- überprüft. **Dr.Web antivirus** Scanner ermöglicht das schnelle oder vollständige Scannen des Dateisystems sowie die Überprüfung einzelner Dateien und Ordner.

Scannen

Führen Sie eine der folgenden Aktionen auf dem Bildschirm **Dr.Web - Scanner** (s. Abbildung 7), um das System zu scannen:

- Um das Scannen installierter Anwendungen zu starten, wählen Sie den Punkt **Schnell**.
- Um das Scannen aller Dateien im System zu starten, wählen Sie den Punkt **Vollständig**.
- Um einzelne Dateien und Ordner zu überprüfen, wählen Sie den Punkt **Benutzerdefiniert**. In der geöffneten Liste mit Objekten des Dateisystems wählen erforderliche Objekte aus (s. Abbildung 8) und drücken Sie die Taste **Prüfen**. Für die Auswahl der Objekte in der Liste können Sie die Optionen benutzen, die sich rechts über der Liste befinden und alle Elemente der Liste wählen bzw. auf die nächste höhere Ebene wechseln, um zwischen den Ordnern zu navigieren.

Nachdem das Scannen beendet wird, erscheint eine Liste entdeckter Bedrohungen auf dem Bildschirm und es wird Ihnen angeboten, Aktionen zur ihren Neutralisierung zu wählen.



Abbildungen 7 und 8. Scanner und Fenster zur Auswahl der Scan-Objekte

Verdächtige Dateien dem Virenlabor von Doctor Web zusenden

Sie können eine verdächtige Datei, die voraussichtlich einen Virus darstellt, bzw. eine offenkundig leere Datei, die einen so genannten "Fehlalarm" auslöst, dem **Virenlabor von Doctor Web** zusenden:

1. Wählen Sie die Datei in der Liste des Dateiverwaltungssystems aus (s. Abbildung 8), klicken Sie danach auf **Dem Virenlabor zusenden**.
2. Geben Sie im nächsten Fenster Ihre e-Mail-Adresse ein, wenn Sie die Ergebnisse der Analyse der zugesandten Datei erhalten möchten.
3. Wählen Sie eine der Kategorien für Ihre Anfrage aus:
   - **Verdacht auf Infizierung**, wenn Sie glauben, dass die Datei eine Bedrohung darstellt;
   - **Fehlalarm** oder **Fehlalarm der Origins Tracing**, wenn Sie glauben, dass die Datei fehlerhaft Bedrohungen zugeordnet wurde.

   Die Auswahl einer der angebotenen Kategorien im Falle des Fehlalarms erfolgt aufgrund des Namens der vermutlich in der zugesandten Datei enthaltenen Bedrohung: Enthält der Name das Suffix «.origin», so sollte die Kategorie **Fehlalarm der Origins Tracing** und in anderen Fällen - die Kategorie **Fehlalarm** gewählt werden.
4. Klicken Sie auf **Senden**.

Dem **Virenlabor von Doctor Web** können Dateien, die nicht größer als 10 MB sind, zugesandt werden.

Scanner konfigurieren

Für den Zugriff auf die Einstellungen von **Dr.Web antivirus** auf dem Haupt- Bildschirm des Programms rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen**. Um den Scanner zu konfigurieren, führen Sie folgende Aktionen auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6) aus:

- Um die Prüfung von Dateien in Archiven zu aktivieren, setzen Sie ein Häkchen bei **Dateien in Archiven** im Bereich **Scanner**.

Standardmäßig ist die Archivprüfung deaktiviert. Durch die Aktivierung der Archivprüfung kann die Operationsgeschwindigkeit des Betriebssystems beschränkt und die Batterielaufzeit reduziert werden. Dabei beeinflusst die Deaktivierung von Archivprüfung den Schutzstatus nicht, da die Installationsdateien für Android-Betriebssystem (.apk) durch den Dateiwächter jedenfalls überprüft werden, unabhängig davon, welcher Wert für diesen Parameter festgelegt wurde.

- um während des Scan-Vorgangs die Pfade der zu überprüfenden Dateien für jeden Kern der Geräte mit Mehrkernprozessoren einzeln anzeigen zu lassen, setzen Sie das Häkchen bei **Anzeige nach Kern** im Abschnitt **Scanner**.
- um die Überprüfung des Systems auf Adware und PUAs (darunter auch Dialer und Scherzprogramme) zu aktivieren/deaktivieren, wählen Sie den Punkt **Optionen** im Bereich **Scanner** und setzen/wählen Sie Häkchen bei **Adware** und **Riskware** ab;
- Um die SD-Karte auf Windows-Autostart-Dateien zu überprüfen, setzen Sie ein Häkchen bei **Autorun-Dateien** im Bereich **Allgemein**. Diese Einstellung wird auch bei Nutzung des Dateiwächters verwendet.

Es ist höchstens empfehlenswert, das Dateisystem regelmäßig zu scannen, z. B. wenn der Wächter einige Zeit nicht aktiv war. In der Regel reicht dabei eine schnelle Systemprüfung aus.

Statistik

Das Programm registriert die Ereignisse, die mit dem Betrieb des Scanners (Prüfungstyp und -ergebnisse, Entdeckung von Sicherheitsbedrohungen) verbunden sind. Die Aktionen des Programms und insbesondere des Scanners werden im Bereich **Aktionen** im Tab **Statistik** nach Datum sortiert angezeigt.

Neutralisierung der Bedrohungen

Liste mit Bedrohungen einsehen

Wenn Sicherheitsbedrohungen durch den **SpIDer Guard** Dateiwächter entdeckt werden, erscheint das Icon im oberen Bereich des Bildschirms. Auf dem Bildschirm wird auch eine Popup-Meldung mit Informationen zu entdeckten Bedrohungen angezeigt. Im Benachrichtigungsbereich klicken Sie auf die Information zu Anzahl entdeckter Bedrohungen, um eine Liste mit allen entdeckten Malware-Objekten zu öffnen.

Bei der Überprüfung Ihres Geräts durch den Scanner öffnet sich die Liste mit entdeckten Bedrohungen automatisch, nachdem der Scanvorgang beendet wird.

Folgende Informationen werden für jede Bedrohung angezeigt:

- Bedrohungsname;
- Pfad der Datei, die eine Bedrohung enthält;
- Bedrohungstyp (Virus, Adware, potentiell unerwünschtes Programm).

Aktionen für Bedrohungen verwenden

Mit **Dr.Web antivirus** kann der Benutzer eine der drei Aktionen für jede entdeckte Bedrohung wählen:

- **Löschen** – die Bedrohung wird aus dem Speicher des Geräts komplett gelöscht
- **In Quarantäne** – die Bedrohung wird in einen speziellen Ordner verschoben und vom System isoliert

Wenn eine Bedrohung in der installierten Anwendung entdeckt wurde, wird es unmöglich sein, sie in die Quarantäne zu verschieben. In diesem Fall fehlt die Aktion **In Quarantäne** in der Liste.

- **Überspringen** – die Anwendung überspringt die Bedrohung und führt keine Aktionen dafür aus
- **Fehlalarm melden** – Es wird Ihnen angeboten, das bedrohliche Objekt dem **Virenlabor von Doctor Web** zusammen mit der Meldung darüber, dass dieses Objekt keine Bedrohung darstellt und fälschlicherweise von dem Antivirusprogramm als verdächtig eingeschätzt wurde, zuzusenden. Um die Ergebnisse der Dateianalyse zu erhalten, geben Sie Ihre E-Mail-Adresse in dem entsprechenden Eingabefeld an und klicken Sie auf **Senden**.

Die Aktion **Fehlalarm melden** ist nur bei Bedrohungsarten mit ".origin" Postfix zugänglich.

Sie können akustische Benachrichtigungen für Entdecken, Löschen und Verschieben von Bedrohungen in Quarantäne einstellen. Dafür auf dem Haupt- Bildschirm des Programms rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen.** Danach setzen Sie ein Häkchen bei **Ton** im Bereich **Allgemein** auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6).

Bedrohungen bei Systemanwendungen entdecken

In manchen Fällen können die Systemanwendungen, die von Herstellern auf Ihr Gerät vorinstalliert werden, Malware-spezifische Funktionen ausführen. Somit kann **Dr.Web antivirus** diese Anwendungen beim Scannen als Sicherheitsbedrohungen beurteilen und eine entsprechende Warnung anzeigen. Die standardmäßigen Aktionen zur Neutralisierung von Bedrohungen können dabei nicht eingesetzt werden. Sie können aber wie folgt vorgehen:

- beenden Sie die Anwendung über die Einstellungen des Geräts (in der Liste installierter Anwendungen auf dem Bildschirm **Einstellungen** -> **Anwendungen** klicken Sie auf den Namen der Anwendung, die als eine Bedrohung beurteilt wurde. Auf dem Bildschirm mit Informationen dazu klicken Sie dann auf **Beenden erzwingen**).

Diesen Vorgang müssen Sie bei jedem Neustart Ihres Geräts wiederholen.

- wenn die Firmware auf Ihrem Gerät verändert wurde, können Sie es auf die Werkseinstellungen zurücksetzen und die Original-Software des Herstellers nutzen;
- wenn Sie die Original-Software des Herstellers von dem mobilen Gerät nutzen, kontaktieren Sie den Hersteller für nähere Informationen zu dieser Anwendung;
- auf einem Gerät mit dem root-Zugriff können Sie es versuchen, die Anwendung mit Hilfe spezieller Tools zu entfernen.

Des Weiteren können Sie die Benachrichtigungen über Bedrohungen, die in bekannten Systemanwendungen erkannt werden, mit Hilfe der Option **Systemanwendungen** im Bereich **Allgemeine Einstellungen** -> **Erweitert** auf dem Bidschirm **Dr.Web - Einstellungen** deaktivieren (s. Abbildung 6).

Sperr-Software bearbeiten

Mit **Dr.Web antivirus** schützen Sie Ihr mobiles Gerät vor weit verbreiteten Ransomware für Android-Plattform. Diese Art von Software ist sehr gefährlich. Damit können die auf Smartphones und Tablet-PCs als Wechseldatenträgern gespeicherten Dateien verschlüsselt werden. Der Bildschirm des mobilen

Geräts kann gesperrt werden, wobei eine Nachricht mit einer Lösegeld-Forderung für Freigabe von Dateien bzw. des Geräts angezeigt wird.

Die Erpresser-Software gefährdet Fotos, Video und Dokumente, die auf der Wechselkarte eines mobilen Geräts gespeichert werden. Darüber hinaus raubt die Ransomware unterschiedliche Informationen zu dem infizierten Gerät (darunter auch IMEI), die Daten aus dem Adressbuch (Kontaktnamen, Rufnummern und E-Mail-Adressen) und übermittelt diese an Server der böswilligen Benutzer. Die ein- und ausgehenden Anrufe werden durch die Ransomware nachverfolgt und können dadurch gesperrt werden. Alle gesammelten Daten, darunter auch über die Anrufe, werden auch an den Verwaltungsserver übermittelt.

Die erpresserische Schadsoftware wird durch **Dr.Web antivirus** erkannt und entfernt, soweit diese versucht, ins geschützte Gerät einzudringen. Die Ransomware wächst aber ständig in Anzahl und Vielfalt. Wenn die **Dr.Web Virendatenbanken** eine gewisse Zeit lang nicht aktualisiert wurden und keine Informationen zu neuen Typen enthalten, kann es vorkommen, dass die Sperr-Software auf dem Gerät installiert wird.

Wenn das mobile Gerät mit dem aktivierten Dateiwächter **SpIDer Guard** durch die Ransomware gesperrt wurde, können Sie wie folgt vorgehen, um das Gerät freizugeben:

1. Schließen Sie Ihr Gerät an ein Ladegerät an und starten Sie die Aufladung.
2. In den folgenden 5 Sekunden schließen Sie das Ladegerät ab.
3. In den folgenden 10 Sekunden schütteln Sie Ihr Gerät energisch.
4. **Dr.Web antivirus** beendet alle aktiven Prozesse auf dem Gerät, eingeschlossen des Prozesses, das durch die Sperr-Software gestartet wurde. Danach ertönt ein kurzes Vibrationssignal (vorausgesetzt, dass diese Funktion auf dem Gerät vorhanden ist). Es öffnet sich der Bildschirm von **Dr.Web antivirus**.

Bitte beachten Sie, dass die Daten anderer Anwendungen beim Beenden der aktiven Prozesse verloren gehen können, wenn diese Anwendungen bei Sperrung des Geräts aktiv waren.

5. Es wird empfohlen, die **Dr.Web Virendatenbanken** nach Freigabe des Geräts zu aktualisieren und eine schnelle Prüfung des Systems durchzuführen bzw. die böswillige Anwendung zu entfernen.

Anruf- und Nachrichtenfilter

Dr.Web antivirus ermöglicht das Filtern von SMS-Nachrichten und Anrufen, indem unerwünschte Nachrichten und Anrufe, z.B. Werbung, sowie Anrufe und Nachrichten von unbekannten Nummern gesperrt werden können.

Für Android 4.4 kann das korrekte Filtern von SMS-Nachrichten gewährleistet werden.

Das Programm bietet die Möglichkeit, den Filtermodus für Anrufe und Nachrichten zu wählen. Außer voreingestellten Profilen, mit denen die Filtermodi festgelegt werden, können auch benutzerdefinierte Profile erstellt werden. Für jedes dieser Profile können eigene Filtereinstellungen festgelegt werden.

Informationen zu gesperrten Anrufen und Nachrichten sind im Bereich **Gesperrte Anrufe und SMS** verfügbar.

Filtermodus wählen

Filtern von Anrufen und Nachrichten erfolgt in einem der folgenden Modi:

- **Alles durchlassen**. In diesem Modus ist Filterung deaktiviert, d.h. alle eingehenden Anrufe und SMS-Nachrichten werden durchgelassen.
- **Alles sperren**. Dabei werden alle eingehenden Anrufe und SMS-Nachrichten gesperrt.
- **Telefonbuch**. In diesem Modus werden eingehende Anrufe und SMS-Nachrichten nur von den ins Telefonbuch eingetragenen Nummern durchgelassen.
- **Blacklist**. In diesem Filtermodus werden Anrufe und SMS-Nachrichten von den in der Blacklist eingetragenen Nummern gesperrt.

Darüber hinaus können Sie einen benutzerdefinierten Filtermodus auswählen. Dieser Filtermodus wird durch das einstellbare Profil festgelegt. **Dr.Web antivirus** erlaubt, eine uneingeschränkte Anzahl von Profilen zu erstellen. Für jedes dieser Profile kann eine Liste der Rufnummern erstellt sowie Aktionen (durchlassen/sperren) für Anrufe und Nachrichten von den Nummern auf dieser Liste festgelegt werden.

Im benutzerdefinierten Filtermodus werden Kontakte auf der Blacklist zusätzlich gesperrt.

Blacklist

Der Blacklist können Nummern, von denen eingehende Anrufe und Nachrichten Sie sperren möchten, hinzugefügt werden. Dabei werden die Anrufe und Nachrichten von den Nummern auf der Blacklist sowie im Filtermodus **Blacklist** als auch bei der Auswahl eines beliebigen benutzerdefinierten Profils zusätzlich zu den Nummern, die auf der Liste dieses Profils sind, gesperrt. Somit wird das Filtern aufgrund der Blacklist nur im Filtermodus **Alles durchlassen** deaktiviert.

Blacklist erstellen

1. Zur Erstellung einer Blacklist tippen Sie auf den Filterbereich auf dem Hauptbildschirm des Programms. Im geöffneten Menü zur Auswahl eines Profils tippen Sie auf **Einstellen**.
2. Im Bereich **Profile/Blacklist** wählen Sie den Tab **Blacklist**.
3. Drücken Sie **Hinzufügen**, um eine Blacklist zu erstellen. Dafür können Sie Kontakte und Rufnummern wie folgt auswählen:
   - aus der Kontaktliste
   - aus dem Anruf- und Nachrichtenlog
   - manuell durch Angeben der Rufnummern und Informationen dazu

   Zur Suche von Kontakten im Telefonbuch sowie in den Anruf- und Nachrichtenlogs können Sie die Suchfunktion nutzen. Dafür drücken Sie die **Suche**-Taste. Sie können jeweils eine bzw. mehrere Rufnummern fürs Hinzufügen zur Blacklist wählen.

   Um ausgewählte Nummern zur Liste hinzuzufügen, drücken Sie die Taste **Hinzufügen**.
4. Für jeden Kontakt auf der Blacklist können Sie eine der folgenden Aktionen wählen:
   - **Anrufe und SMS sperren** – um alle eingehenden Anrufe und Nachrichten von diesem Kontakt zu sperren
   - **Nur Anrufe sperren** – um nur eingehende Anrufe von einem bestimmten Kontakt zu sperren. Die Nachrichten werden dabei durchgelassen
   - **Nur SMS sperren** – um nur Nachrichten, die von einem bestimmten Kontakt eingehen, zu sperren. Die Anrufe werden dabei durchgelassen

Standardmäßig wird die Aktion **Anrufe und SMS sperren** für jeden hinzugefügten Kontakt festgelegt. Gegebenenfalls können Sie diese Einstellung ändern.

5. Um Angaben eines Kontakts auf der Blacklist zu ändern, tippen Sie darauf und halten Sie den Kontakt gedrückt bzw. streichen Sie den Kontakt nach links oder rechts. Im geöffneten Menü tippen Sie auf **Editieren**. Bearbeiten Sie die Felder **Name** und **Nummer**. Drücken Sie die Taste **Speichern**.

Die Angaben der Kontakte aus dem Telefonbuch sowie der privaten Nummern können nicht bearbeitet werden.

6. Um eine Nummer aus der Blacklist zu entfernen, tippen Sie darauf und halten Sie die Nummer gedrückt bzw. streichen Sie sie nach rechts oder links. Im geöffneten Menü tippen Sie auf **Löschen**.
7. Sie können auch eine Liste der Schlagwörter erstellen, damit alle SMS-Nachrichten, die solche Schlagwörter enthalten, gesperrt werden. Dafür wählen Sie die Option **Schlagwort** im Menü, das Optionen fürs Hinzufügen der Kontakte zur Blacklist bietet. Im Bereich **SMS Sperrung nach Schlagwörtern** geben Sie ein Schlagwort ein und drücken Sie die Taste **Hinzufügen**.

Blacklist bereinigen

Um alle Kontakte aus der Blacklist zu entfernen, drücken Sie die **Menü**-Taste und wählen Sie den Punkt **Liste leeren**.

Filterprofil erstellen

Dr.Web antivirus ermöglicht die Erstellung benutzerdefinierter Filtermodi für Anrufe und Nachrichten.

Neues Profil erstellen

1. In der Liste verfügbarer Profile drücken Sie **Einstellen**.
2. Im Tab **Profile** auf dem Bildschirm **Profile/Blacklist** drücken Sie die Taste **Profil hinzufügen**. Es öffnet sich der Bereich **Profil hinzufügen**.
3. Geben Sie den Profilnamen ein.
4. Wählen Sie eine Aktion für eingehende Anrufe und Nachrichten von den Nummern, die auf der Liste in diesem Profil sind. Folgende Aktionen sind verfügbar:
   - **Nur Kontakte aus der Liste erlauben** – damit Anrufe und Nachrichten nur von den Nummern, die auf der Liste in diesem Profil sind, durchgelassen werden
   - **Kontakte aus der Liste sperren** – damit Anrufe und Nachrichten von den Nummern, die auf der Liste in diesem Profil sind, gesperrt werden
5. Drücken Sie **Kontakt hinzufügen**, um eine Kontaktliste zu erstellen. Sie können die Nummern wie folgt auswählen:
   - aus der Kontaktliste
   - aus Anruf- und Nachrichtenlogs
   - manuell durch Eingabe der Rufnummern und Informationen dazu

   Zur Suche von Kontakten im Telefonbuch sowie in den Anruf- und Nachrichtenlogs können Sie die Suchfunktion nutzen. Dafür drücken Sie die **Suche**-Taste. Sie können jeweils eine bzw. mehrere Rufnummern fürs Hinzufügen zur Profilliste wählen.

   Um ausgewählte Nummern zur Liste hinzuzufügen, drücken Sie die Taste **Hinzufügen**. Die Anzahl der Kontakte auf der Profilliste wird neben dem Profilnamen rechts in Klammern angezeigt.

Die Kontaktliste des Profils kann nicht leer sein.

6. Um Angaben eines Kontakts auf der Liste zu ändern, tippen Sie darauf und halten Sie den Kontakt gedrückt bzw. streichen Sie den Kontakt nach rechts oder links. Im geöffneten Menü tippen Sie auf **Editieren**. Bearbeiten Sie die Felder **Name** und **Nummer**. Drücken Sie die Taste **Speichern**.

Die Angaben der Kontakte aus dem Telefonbuch sowie der privaten Nummern können nicht bearbeitet werden.

7. Um einen Kontakt aus der Profilliste zu entfernen, tippen Sie darauf und halten Sie den Kontakt gedrückt bzw. streichen Sie nach rechts oder links. Im geöffneten Menü tippen Sie auf **Löschen**.

Die aus einem benutzerdefinierten Profil gelöschten Kontakte bleiben in der Kontaktliste des Telefonbuches erhalten.

Gesperrte Anrufe und Nachrichten einsehen

Auf dem Hauptbildschirm des Programms wird die Anzahl gesperrter Anrufe und Nachrichten im Filterbereich angezeigt. Um die Listen gesperrter Anrufe und Nachrichten einzusehen, tippen Sie auf das entsprechende Symbol:

- – um gesperrte Anrufe einzusehen
- – um gesperrte Nachrichten einzusehen

Neben den Listennamen rechts wird die Anzahl der nicht eingesehenen Anrufe/Nachrichten in Klammern angezeigt. Für jeden Anruf/jede Nachricht auf der Liste werden folgende Informationen angezeigt:

- Datum und Uhrzeit des eingehenden Anrufs/der eingehenden Nachricht
- Rufnummer und Name des Anrufers/SMS-Absenders

Aktionen für gesperrte Anrufe/Nachrichten

1. Sie können den Anrufer, dessen Anruf gesperrt wurde, zurückrufen. Dafür tippen Sie auf den Anruf in der Liste. Es öffnet sich der Bildschirm mit gewählter Rufnummer. Um Anruf zu tätigen, tippen Sie auf **Anrufen**.
2. Beim Tippen auf eine Nachricht auf der Liste gesperrter Nachrichten öffnet sich der Text sowie die Angaben der Nachricht. Es wird Ihnen auch angeboten, eine der folgenden Aktionen dafür zu wählen:
   - **Wiederherstellen** – damit die Nachricht in die Liste eingehender Nachrichten verschoben wird
   - **Löschen** – damit die Nachricht gelöscht wird

Virendatenbanken aktualisieren

Zur Entdeckung von Sicherheitsbedrohungen nutzt **Dr.Web antivirus** spezielle **Virendatenbanken von Dr.Web**, die Angaben über alle den Spezialisten von **Doctor Web** bekannten Informationsbedrohungen für mobile Geräte enthalten. Die Datenbanken bedürfen einer regelmäßigen Aktualisierung, da immer neue Schadprogramme erscheinen können. Dafür können die Virendatenbanken über Internet aktualisiert werden.

Auf dem Hauptbildschirm des Programms wird das Datum der letzten Aktualisierung im Bereich **Update** angezeigt.

Aktualisierung

1. Zur Aktualisierung von Virendatenbanken tippen Sie auf den Bereich mit Informationen zu Updates auf dem Haupt- Bildschirm des Programms.
2. Die Aktualisierung wird automatisch gestartet.

Es empfiehlt sich, die Virendatenbanken gleich nach der Installation des Programms zu aktualisieren, damit **Dr.Web antivirus** die aktuellsten Informationen zu bekannten Bedrohungen nutzen kann. Die Virensignaturen, Informationen zu deren Merkmalen und Verhaltensmustern werden sofort aktualisiert, sobald neue Bedrohungen durch Spezialisten des **Virenlabors von Doctor Web** entdeckt werden. Manchmal kann es mehrmals pro Stunde passieren. Manchmal geschieht dies mehrmals pro Stunde.

Aktualisierungseinstellungen

Standardmäßig werden die Updates automatisch vier Mal am Tag geladen. In dem Bereich **Update** auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6) können Sie die Verwendung von mobilen Netzwerken beim Herunterladen von Updates erlauben/verbieten. Damit keine mobilen Netzwerke beim Herunterladen von Updates benutzt werden, setzen Sie ein Häkchen bei **Mobiles Internet nicht benutzen**. Wenn keine aktiven Netzwerke entdeckt werden, wird es Ihnen angeboten, 3G- bzw. GPRS-Netze zu nutzen.

Bei der Aktualisierung werden die Daten übers Netzwerk geladen. Für die Datenübertragung können zusätzliche Kosten anfallen. Mehr dazu fragen Sie bei Ihrem Mobilfunkanbieter.

Mit Quarantäne arbeiten

Entdeckte Bedrohungen werden durch **Dr.Web antivirus** in Quarantäne – in einen speziellen Ordner, der zur deren Isolierung und sicheren Speicherung dient – verschoben.

Bedrohungen in Quarantäne behandeln

1. Zum Einsehen einer Liste der in die Quarantäne verschobenen Bedrohungen auf dem Haupt-Bildschirm des Programms wählen Sie den Punkt **Quarantäne**.
2. Es öffnet sich die Liste aller Bedrohungen, die sich in der Quarantäne befinden (s. Abbildung 9).
3. Tippen Sie auf eine Bedrohung in der Liste, um folgende Informationen dazu einzusehen:
   - Dateiname
   - Pfad der Datei
   - Datum der Verschiebung in die Quarantäne

   Darüber hinaus können Sie dem Link im Bereich **Informationen im Internet** folgen, um weitere Informationen zu ähnlichen Bedrohungen im Internet auf der Website von **Doctor Web** einzusehen.

4. Sie können eine der folgenden Aktionen für jede Bedrohung ausführen:
   - **Wiederherstellen** – um die Datei in den Ordner, in dem sich diese Datei vor ihrer Verschiebung befand, zu bringen (verwenden Sie diese Funktion nur in dem Fall, wenn es kein Zweifel besteht, dass die Datei sicher ist)
   - **Löschen** – um die Datei aus der Quarantäne und aus dem System zu löschen
   - **Fehlalarm melden** – um die Datei dem **Virenlabor von Doctor Web** zuzusenden sowie zu informieren, dass diese keine Bedrohung darstellt und vom Antivirusprogramm fälschlicherweise als verdächtig eingeschätzt wurde. Um die Ergebnisse der Virenanalyse für die zugeschickte Datei zu erhalten, geben Sie Ihre E-Mail-Adresse in dem entsprechenden Eingabefeld an und klicken Sie auf **Senden**.

Abbildung 9. Quarantäne

Größe von Quarantäne

Sie können Informationen zum Speicherplatz, der durch Quarantäne eingenommen wird, sowie zum freien Speicherplatz auf der SD-Karte einsehen. Dafür rufen Sie das Anwendungsmenü im Tab **Quarantäne** und wählen Sie den Punkt **Quarantäne-Größe**.

Statistik

Dr.Web antivirus ermöglicht die Führung der Statistik über entdeckte Bedrohungen und Aktionen des Programms. Um Statistiken über die Funktion des Programms einzusehen, auf dem Haupt- Bildschirm des Programms wählen Sie den Punkt **Statistik**.

Im **Statistik**-Tab finden Sie zwei Informationsbereiche (s. Abbildung 10):

- **Insgesamt**-Bereich, der Informationen zur Gesamtzahl überprüfter Dateien, entdeckter und neutralisierter Bedrohungen beinhaltet
- **Aktionen**-Bereich, der Informationen zu Prüfungsbeginn/-Ende, Aktivierung/Deaktivierung des Wächters sowie zu entdeckten Bedrohungen und Aktionen zu deren Neutralisierung beinhaltet

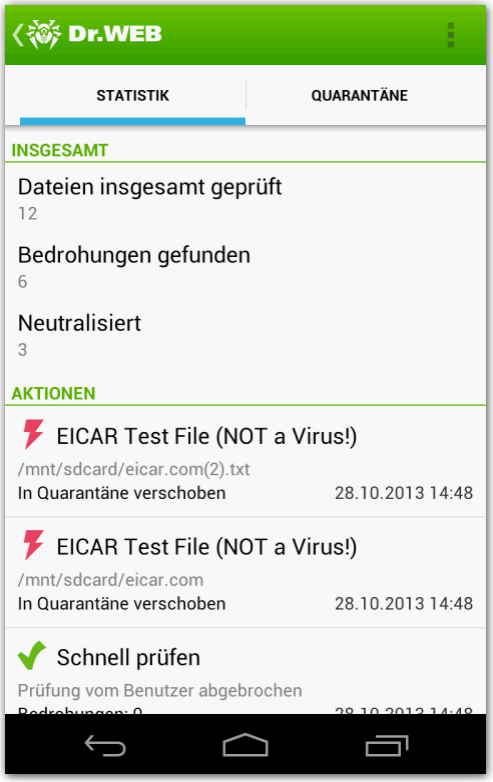


Abbildung 10. Statistik

Statistik bereinigen

Um alle gesammelten Statistiken über die Funktion des Programms zu löschen, rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Statistik löschen**.

Ereignislog

Das Programm ermöglicht Führung von einem Ereignislog, das auf der SD-Karte gespeichert und an technischen Support von **Doctor Web** gesendet wird, falls Probleme bei der Nutzung der Anwendung entstehen.

Um das Ereignislog zu speichern:

1. Drücken Sie die **Menü**-Taste im **Statistik**-Tab und wählen Sie den Punkt **Protokoll speichern**.
2. Das Log wird in der Datei DrWeb_Log.txt gespeichert. Diese Datei befindet sich im Verzeichnis Android/data/com.drweb/files auf der SD-Karte.

Dr.Web Anti-Theft

Dr.Web Anti-Theft hilft Ihnen, Ihr Telefon beim Verlust oder Diebstahl zu orten bzw. seine Funktionen sofort zu sperren.

Dr.Web Anti-Theft wird mit speziellen SMS-Befehlen verwaltet. Für den Zugriff auf die Einstellungen von **Dr.Web Anti-Theft** ist ein spezielles Passwort einzugeben, das bei der Ersteinstellung festgelegt wird. Dieses Passwort müssen Sie sich merken, da alle Funktionen von **Dr.Web Anti-Theft** damit gesteuert werden sowie Sie werden es fürs Entsperren Ihres Gerätes brauchen, falls es gesperrt wird. Wenn Sie das für **Dr.Web Anti-Theft** festgelegte Passwort vergessen haben, können Sie speziellen Service zur Zurücksetzung des Passworts und Freigabe Ihres Gerätes nutzen.

Darüber hinaus können Sie mit **Dr.Web Anti-Theft** eine Freundesliste (bis zu 5 Telefonnummern) erstellen. Von Telefonnummern ihrer Freunde wird es möglich sein, SMS-Befehle auch dann zu senden, wenn Sie Ihr Passwort für **Dr.Web Anti-Theft** vergessen.

Ersteinstellung

Beim ersten Start von **Dr.Web Anti-Theft** öffnet sich das Fenster mit dem Einstellungsassistenten, mit dem Sie die Grundfunktionen einstellen können:

- Drücken Sie **Weiter**, um zur Einstellung der Grundfunktionen von **Dr.Web Anti-Theft** zu wechseln.
- Drücken Sie **Abbrechen**, wenn Sie **Dr.Web Anti-Theft** später konfigurieren wollen.

Ersteinstellung von Dr.Web Anti-Theft mit dem Einstellungsassistenten

1. Im ersten Einstellungsschritt von **Dr.Web Anti-Theft** legen Sie ein Passwort fest (das Passwort muss mindestens 4 Zeichen enthalten). Dieses Passwort dient zur Steuerung aller Funktionen von **Dr.Web Anti-Theft**. Gegebenenfalls aktivieren Sie die Option Zeichen bei Passworteingabe anzeigen. Dazu drücken Sie das Symbol rechts neben dem Eingabefeld. Um das Passwort auszublenden, drücken Sie das Symbol . Tippen Sie auf **Weiter**.
2. Bestätigen Sie das eingegebene Passwort. Drücken Sie **OK**.
3. Konfigurieren Sie die Freundesliste. Tippen Sie auf **Weiter**.
4. Wenn Sie bisher kein Google-Konto angelegt haben, öffnet sich im weiteren Verlauf ein Eingabefeld zur Angabe Ihrer E-Mail-Adresse, um **Dr.Web Anti-Theft** auf dem Server von **Doctor Web** zu registrieren. Dies ist notwendig, um Ihnen bei Bedarf den Code zur Entsperrung des Telefons bzw. zur Eingabe eines neuen Passworts zuzusenden, falls Sie das Passwort für **Dr.Web Anti-Theft** vergessen sollten. Geben Sie eine gültige E-Mail-Adresse an und klicken Sie auf **Weiter**.

   Um Ihre E-Mail-Adresse auf dem Server zu registrieren, benötigen Sie eine aktive Internetverbindung.

5. Geben Sie einen Text ein, der auf dem Bildschirm Ihres Telefons im Fall seiner Sperrung angezeigt wird. Tippen Sie auf **Weiter**.
6. Die erstmalige Einstellung von **Dr.Web Anti-Theft** ist damit abgeschlossen. Es wird Ihnen angeboten, die bei der Anmeldung Ihres Google-Kontos angegebene E-Mail-Adresse (bzw. die im vorhergehenden Eistellungsschritt angegebene E-Mail-Adresse) auf dem Server von **Doctor Web** zu registrieren. Klicken Sie auf **Fertig**, um die Registrierung zu starten:
   - bei einer erfolgreichen Registrierung wird der Einstellungsassistent geschlossen und das Dialogfenster **Dr.Web - Anti-Theft** (s. Abbildung 11) wird geöffnet;
   - sollten bei der Registrierung Probleme auftreten, erscheint auf dem Bildschirm die Meldung mit der Fehlerbeschreibung. Dabei erfolgt keine Aktivierung von **Dr.Web Anti-Theft** auf Ihrem Gerät.

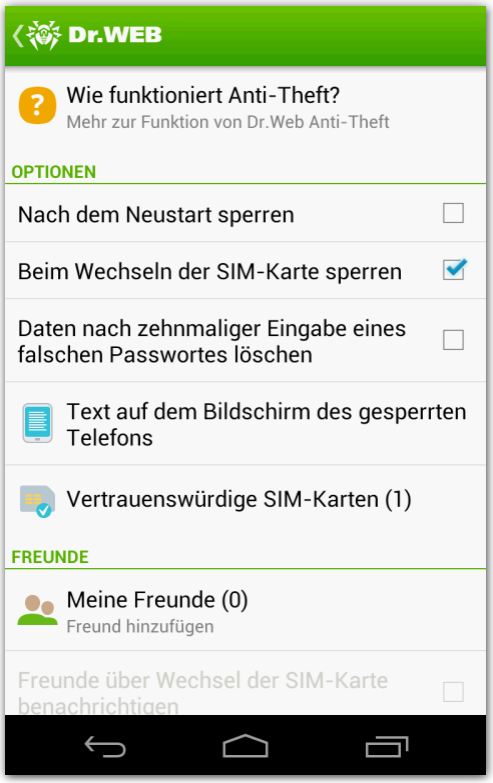


Abbildung 11. Bildschirm Dr.Web - Anti-Theft.

Beim Wechseln zum Hauptbildschirm mit Einstellungen von **Dr.Web Anti-Theft** kann eine Nachricht auftauchen, in der es Ihnen angeboten wird, **Dr.Web antivirus** als Geräteadministrator festzulegen. Sie haben diese Anforderung zu akzeptieren, damit **Dr.Web Anti-Theft** vollwertig funktionieren kann.

Hilfe aufrufen

Um Hilfe für **Dr.Web Anti-Theft** aufzurufen, wählen Sie den Punkt **Wie funktioniert Anti-Theft?** im **Hilfe**-Bereich auf dem Bildschirm **Dr.Web - Anti-Theft** (s. Abbildung 11).

Passwort ändern

Um das für **Dr.Web Anti-Theft** festgelegte Passwort zu ändern, gehen Sie auf dem Bildschirm **Dr.Web - Anti-Theft** (s. Abbildung 11) wie folgt vor:

1. Im Bereich **Passwort und Administrieren** drücken Sie **Passwort ändern**.
2. Geben Sie aktuelles Passwort ein. Drücken Sie **OK**.
3. Geben Sie ein neues Passwort ein. Tippen Sie auf **Weiter**.
4. Bestätigen Sie das neue Passwort. Drücken Sie **OK**.

Neue E-Mail-Adresse registrieren

Um die für **Dr.Web Anti-Theft** auf dem Server von **Doctor Web** registrierte E-Mail-Adresse zu ändern, wählen Sie folgende Aktionen im Dialogfenster **Dr.Web - Anti-Theft** (s. Abbildung 11):

1. Im Abschnitt **Passwort und Administrieren** klicken Sie auf **E-Mail-Adresse ändern**.
2. Geben Sie die E-Mail-Adresse für die Registrierung auf dem Server von **Doctor Web** ein. Klicken Sie auf **OK**.
3. Eine E-Mail mit der Bestätigung der durchgeführten Änderungen wird an die erstangemeldete E-Mail-Adresse geschickt.

Deaktivierung von Dr.Web Anti-Theft

Um **Dr.Web Anti-Theft** auf Ihrem Gerät zu deaktivieren, wählen Sie folgende Aktionen im Dialogfenster **Dr.Web - Anti-Theft** (s. Abbildung 11):

1. Im Abschnitt **Passwort und Administrieren** klicken Sie auf **Dr.Web Anti-Theft deaktivieren**.
2. Geben Sie Ihr für **Dr.Web Anti-Theft** registriertes Passwort ein und klicken Sie auf **Dr.Web Anti-Theft deaktivieren**.

Bei Deaktivierung von **Dr.Web Anti-Theft** wird das Sicherheitsniveau wesentlich verringert!

Optionen einstellen

Um **Dr.Web Anti-Theft** zu konfigurieren, wählen Sie den **Anti-Theft**-Bereich auf dem Hauptbildschirm der Anwendung. Für den Zugang zum Bildschirm mit Einstellungen für **Dr.Web Anti-Theft** müssen Sie das für **Dr.Web Anti-Theft** beim ersten Start festgelegte Passwort eingeben. Wenn Sie das Passwort vergessen haben, senden Sie den SMS-Befehl **#RESETPASSWORD#** von einer Rufnummer, die auf Ihrer Freundesliste ist, an Ihr Gerät bzw. nutzen Sie den speziellen Service.

Optionen

Um **Dr.Web Anti-Theft** zu konfigurieren, gehen Sie im Bereich **Optionen** auf dem Bildschirm **Dr.Web - Anti-Theft** (s. Abbildung 11) wie folgt vor:

- Um das Telefon im Falle seines Neustarts zu sperren, aktivieren Sie die Option **Nach dem Neustart sperren**.
- Damit Ihr Telefon bei SIM-Kartenwechsel gesperrt wird, aktivieren Sie die Option **Beim Wechseln der SIM-Karte sperren**.
- Damit ihre persönlichen Daten auf der SD-Karte nach 10-maliger falscher Passworteingabe vollständig gelöscht werden, aktivieren Sie die Option **Daten nach zehnmaliger Eingabe eines falschen Passwortes löschen**.
- Um den Text, der auf dem Bildschirm des gesperrten Telefons angezeigt wird, festzulegen, drücken Sie **Text auf dem Bildschirm des gesperrten Telefons** und geben Sie den Text ein (Sie können zum Beispiel Ihre Kontaktdaten angeben, damit man das gefundene Telefon Ihnen zurückgeben konnte). Danach drücken Sie die **Speichern**-Taste.
- Um die Liste mit vertrauenswürdigen SIM-Karten einzusehen und zu bearbeiten, tippen Sie auf **Vertrauenswürdige SIM-Karten**.

Vertrauenswürdige SIM-Karten

SIM-Karten, die in Ihrem mobilen Gerät genutzt werden, können der Liste vertrauenswürdiger SIM-Karten von **Dr.Web Anti-Theft** hinzugefügt werden. Wird eine vertrauenswürdige SIM-Karte auf dieser Liste durch eine andere ersetzt, wird Ihr Gerät durch **Dr.Web Anti-Theft** nicht gesperrt. Neue SIM-Karten werden zur Liste beim Neustart des Geräts bzw. beim Start von **Dr.Web antivirus** hinzugefügt. Sie können auch den Betrieb ohne SIM-Karte zu dieser Liste hinzufügen.

Der Betrieb ohne SIM-Karte kann aktiviert werden, wenn keine SIM-Karte in Ihrem Gerät installiert ist sowie auch wenn Ihr Gerät keinen Zugriff auf die Information über SIM-Karte den installierten Anwendungen erlaubt. Dadurch können Sie eine Fehlermeldung über eine fehlende SIM-Karte erhalten. Wenn aber Sie einen solchen Betriebsmodus als vertrauenswürdig festlegen, werden alle Funktionen von **Dr.Web Anti-Theft** im vollen Umfang für Sie zugägnglich sein.

Zum Einsehen und Bearbeiten der Liste von vertrauenswürdigen SIM-Karten drücken Sie **Vertrauenswürdige SIM-Karten** im Bereich Optionen von **Dr.Web Anti-Theft**:

1. Standardsmäßig werden hinzugefügte SIM-Karten SIM1, SIM2 usw. genannt. Um einen neuen Namen einer SIM-Karte zu geben, tippen Sie auf deren Namen in der Liste (bzw. drücken Sie den Namen und halten Sie gedrückt, im geöffneten Menü wählen Sie **Editieren** aus). Es öffnet sich ein Fenster mit Information zu SIM-Karte. Geben Sie hier einen neuen Namen im Feld **Vorname** ein und tippen Sie auf **Speichern**.
2. Um eine SIM-Karte aus der Liste vertrauenswürdiger SIM-Karten zu löschen, drücken Sie und halten Sie ihren Namen gedrückt. Im geöffneten Menü wählen Sie **Löschen** aus.

Die in Ihrem Gerät aktuell genutzte SIM-Karte kann aus der Liste vertrauenswürdiger SIM-Karten nicht gelöscht werden.

Freundesliste

Dr.Web Anti-Theft ermöglicht das Hinzufügen von bis zu 5 Rufnummern zur Freundesliste. Für diese Rufnummern können Sie Versand von SMS-Befehlen an Ihr Telefon ohne Passworteingabe einstellen. Darüber hinaus können Sie einen SMS-Befehl zur Deaktivierung von **Dr.Web Anti-Theft** und Zurücksetzung des dafür festgelegten Passworts von diesen Rufnummern senden.

Freundesliste konfigurieren

1. Auf dem Bildschirm **Dr.Web - Anti-Theft** (s. Abbildung 11) im **Freunde**-Bereich drücken Sie **Meine Freunde**.
2. Drücken Sie **Hinzufügen**, um Freundesliste zu erstellen. Sie können Kontakte und Rufnummern wie folgt auswählen:
   - aus der Kontaktliste
   - aus dem Anruf- und Nachrichtenlog
   - manuell durch Eingabe von Rufnummern und Informationen dazu

   Zur Suche von Kontakten im Telefonbuch sowie in den Anruf- und Nachrichtenlogs können Sie die Suchfunktion nutzen. Dafür drücken Sie die **Suche**-Taste. Sie können jeweils eine bzw. mehrere Rufnummern fürs Hinzufügen zur Blacklist wählen.

   Um ausgewählte Nummern zur Liste hinzuzufügen, drücken Sie die Taste **Hinzufügen**.
3. Um Angaben eines Kontakts auf der Liste zu ändern, drücken Sie darauf in der Liste und bearbeiten Sie die Werte in den Feldern **Name** und **Nummer** auf dem Bildschirm **Kontakt editieren**. Drücken Sie die Taste **Speichern**.
4. Um eine Nummer aus der Liste zu entfernen, drücken Sie diese Nummer und halten Sie sie gedrückt. Im geöffneten Menü tippen Sie auf **Löschen**.
5. Um Ihre Freunde über den SIM-Kartenwechsel auf Ihrem Telefon zu benachrichtigen, aktivieren Sie die Option **Freunde über Wechsel der SIM-Karte benachrichtigen**.
6. Damit der Versand von SMS-Befehlen von Rufnummern Ihrer Freunde ohne Eingabe des für **Dr.Web Anti-Theft** festgelegten Passworts erlaubt wird, aktivieren Sie die Option **SMS-Befehle ohne Passwort erlauben**.

Unabhängig davon, ob die Option **SMS-Befehle ohne Passwort erlauben** gewählt ist oder nicht, können Ihre Freunde den Befehl #RESETPASSWORD# ohne Passwort an Ihr Telefon senden. Dieser Befehl dient zur Freischaltung des Telefons und Zurücksetzung des Passworts für **Dr.Web Anti-Theft**.

SMS-Befehle

Die Verwaltung von **Dr.Web Anti-Theft** erfolgt über spezielle SMS-Befehle. Diese Befehle ermöglichen es Ihnen, Ihr Telefon zu orten sowie seine Funktionen zu sperren und Ihre persönliche Daten zu löschen.

Tabelle der SMS-Befehle

Zur Verwaltung von **Dr.Web Anti-Theft** können Sie folgende SMS-Befehle verwenden:

Befehl	Aktion
#SIGNAL#*Passwort#*	Telefon sperren und ein Tonsignal darauf aktivieren, das auch nach dem Neustart des Telefons erklingen wird.
#LOCK#*Passwort#*	Telefon sperren.
#UNLOCK#*Passwort#*	Telefon ohne Zurücksetzung des Passworts für **Dr.Web Anti-Theft** freischalten.
#LOCATE#*Passwort#*	GPS-Koordinaten des Telefons in einer SMS-Nachricht erhalten. Die erhaltene SMS-Nachricht wird einen Link zur Karte mit vermutlichen Koordinaten Ihres Geräts beinhalten. Wenn Sie dem erhaltenen Link folgen, wird der Standort Ihres Geräts mit Hilfe von **Dr.Web Anti-theft Locator** angezeigt. Es ist ein spezieller Dienst von **Doctor Web**, der eine Karte und den Standort Ihres Geräts darauf im Fenster des Webbrowsers anzeigen lässt. Die Genauigkeit bei Ortung des Geräts hängt von verfügbaren GPS-Empfängern, sichtbaren Wi-Fi-Netzwerken sowie von den nächstgelegenen GSM-Basissendestationen ab. Je nach erhaltenen Daten wird der Standort genau (als eine Position auf der Karte) bzw. ungefähr (als ein Kreis bestimmter Größe) bestimmt. Im oberen Bereich des Bildschirms mit Karte können Sie den gewünschten Ortungsdienst wählen.
#WIPE#*Passwort#*	Telefon auf die Werkseinstellungen zurücksetzen und alle Daten von der SD-Karte löschen. Dieser Befehl wird auch nach 10-maliger falscher Passworteingabe ausgeführt, falls das Telefon gesperrt ist und die Option **Daten nach zehnmaliger Eingabe eines falschen Passwortes löschen** in den Einstellungen von **Dr.Web Anti-Theft** ausgewählt wurde.
#RESETPASSWORD#	Telefon freischalten und das für **Dr.Web Anti-Theft** festgelegte Passwort zurücksetzen. Dieser Befehl kann nur von einer Rufnummer, die auf der Freundesliste ist, gesendet werden.

SMS-Befehle sind nicht schreibungsabhängig. Beispielsweise können Sie den Befehl **#LOCK#***Passwort#* in Form von **#Lock#***Passwort#*, **#lock#***Passwort#*, **#lOck#***Passwort#* usw. senden, um das Telefon zu sperren.

Zur Genauigkeit der nach dem Versand des SMS-Befehls #LOCATE# erhaltenen Ergebnisse erlauben Sie die Nutzung drahtloser Netzwerke in den Einstellungen Ihres Gerätes bei seiner Ortung.

SMS-Befehle über die Oberfläche von Dr.Web Anti-Theft senden

Sie können SMS-Befehle direkt über die Oberfläche von **Dr.Web Anti-Theft** an andere Telefone, die auch mit **Dr.Web Anti-Theft** eingerichtet sind, versenden. Dafür müssen Sie wie folgt vorgehen:

1. Auf dem Bildschirm **Dr.Web - Anti-Theft** (s. Abbildung 11) im Bereich **Freunde** drücken Sie **SMS-Befehle senden**.
2. Geben Sie die Rufnummer ein, an die Sie einen SMS-Befehl senden wollen.
3. Wählen Sie einen Befehl aus der Liste aus:
   - **Sperren** – entspricht dem Befehl #LOCK#
   - **Sperren und Tonsignal aktivieren** – entspricht dem Befehl #SIGNAL#

- **Freischalten** – entspricht dem Befehl #UNLOCK#
- **Alle Daten löschen** – entspricht dem Befehl #WIPE#
- **Lage feststellen** – entspricht dem Befehl #LOCATE#
- **Passwort zurücksetzen** – entspricht dem Befehl #RESETPASSWORD#

4. Geben Sie das für **Dr.Web Anti-Theft** auf dem Telefon des Befehlsempfängers festgelegte Passwort ein. Wenn Ihre Rufnummer der Freundesliste des Befehlsempfängers hinzugefügt ist, brauchen Sie nicht, das Passwort einzugeben.
5. Tippen Sie auf **Senden**.

Passwort wiederherstellen

Sollten Sie Ihr für **Dr.Web Anti-Theft** definiertes Passwort vergessen haben, führen Sie folgende Aktionen aus:

1. Öffnen Sie die Internetseite **Verfahren zum Erhalten des Deaktivierungscodes für Dr.Web Anti-Theft** unter https://antitheft.drweb.com/.
2. Geben Sie den Code ein, der auf dem Bildschirm des gesperrten Gerätes erscheint, sowie die E-Mail-Adresse, die zur Registrierung von **Dr.Web Anti-Theft** auf dem Server von **Doctor Web** genutzt wurde, in entsprechenden Feldern ein.
3. Klicken Sie auf **Send code**. Ein spezieller Code zur Entsperrung des Gerätes und zur Deaktivierung von **Dr.Web Anti-Theft** wird an die angegebene E-Mail-Adresse gesendet. Geben Sie bitte diesen Code in das Passwortfeld auf dem Bildschirm des gesperrten Gerätes ein. Daraufhin wird **Dr.Web Anti-Theft** deaktiviert. Um **Dr.Web Anti-Theft** erneut zu aktivieren, müssen Sie das Programm neu starten und notwendige Einstellungen vornehmen.

Zugriff auf Internet-Inhalte einschränken

Zugriff auf Internet-Inhalte wird mit einem speziellen URL-Filter **Cloud Checker** kontrolliert. Damit wird der Benutzer des mobilen Geräts vor unerwünschten Webinhalten geschützt.

Mit **Cloud Checker** wird der Zugriff auf Webinhalte nur beim integrierten Android-Browser sowie dem Browser Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser bzw. Boat Browser Mini kontrolliert.

Mit Hilfe von **Cloud Checker** kann der Zugriff auf unterschiedliche Kategorien nicht empfohlener und potentiell gefährlicher Websites gesperrt werden:

- Chats
- Drogen
- E-Mail
- Glücksspiele
- Bekannte Viren-Quellen
- Anstößige Sprache
- Soziale Netzwerke
- Terrorismus
- Gewalt
- Waffen
- Websites für Erwachsene
- Nicht empfohlene Websites

URL-Filter aktivieren/deaktivierens

1. Auf dem Hauptbildschirm der Anwendung (s. Abbildung 2) wählen Sie **Cloud Checker**. Es öffnet sich der Bildschirm mit Einstellungen für den URL-Filter (s. Abbildung 12).

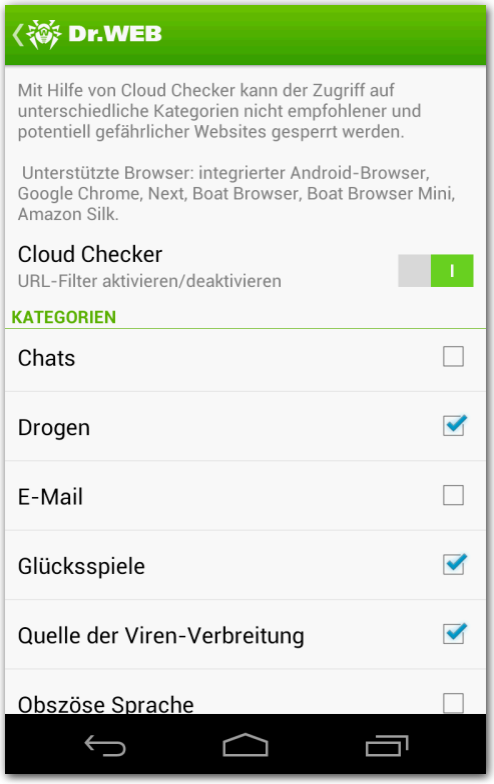

Dr.WEB
Mit Hilfe von Cloud Checker kann der Zugriff auf unterschiedliche Kategorien nicht empfohlener und potentiell gefährlicher Websites gesperrt werden.
Unterstützte Browser: integrierter Android-Browser, Google Chrome, Next, Boat Browser, Boat Browser Mini, Amazon Silk.
Cloud Checker
URL-Filter aktivieren/deaktivieren
KATEGORIEN
Chats
Drogen
E-Mail
Glücksspiele
Quelle der Viren-Verbreitung
Obszöse Sprache

Abbildung 12. Bildschirm mit Einstellungen für Cloud Checker.

2. Filtern der Internet-Inhalte wird mit Option **Cloud Checker** aktiviert/deaktiviert. Standardsmäßig ist Filtern der Internet-Inhalte aktiv.
3. In der Liste **Kategorien** wählen Sie die Kategorien von Websites aus, auf welche Sie den Zugriff sperren wollen.

Dr.Web Firewall

Dr.Web Firewall ist für den Schutz Ihres mobilen Geräts vor unbefugtem Zugang von außen bestimmt und beugt dem Verlust wichtiger Daten im Netzwerk vor. Diese Komponente gestattet es Ihnen, die Verbindungen und Datenübertragung im Internet zu überwachen sowie verdächtige Verbindungen zu sperren.

Dr.Web Firewall nutzt die VPN-Technologie für Android. Bei manchen Geräten kann das VPN-Protokoll vom Hersteller deaktiviert werden und für andere Anwendungen nicht zugänglich sein. In diesem Fall sind die Firewall-Funktionen nicht verfügbar. Für weitere Informationen kontaktieren Sie den Hersteller Ihres mobilen Geräts.

Dr.Web Firewall aktivieren/deaktivieren

1. Auf dem Hauptbildschirm der Anwendung (s. Abbildung 2) wählen Sie die Option **Firewall**. Es öffnet sich der Einstellungsbildschirm der Firewall (s. Abbildung 13).

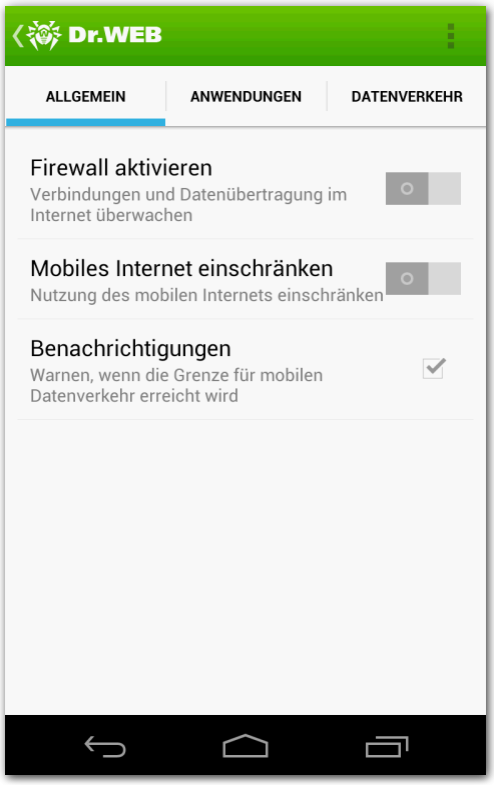


Abbildung 13. Einstellungsbildschirm der Firewall. Registerkarte Allgemein.

2. Das Aktivieren/Deaktivieren der Firewall erfolgt mit Hilfe der Option **Firewall aktivieren**. Standardgemäß ist die Firewall deaktiviert. Beim Aktivieren der Firewall wird der Benutzer angefordert, die VPN-Verbindungen für **Dr.Web antivirus Antivirus** freizugeben. Sie müssen VPN erlauben, damit die Firewall funktioniert.

Wenn die Rechte für die VPN-Nutzung im Laufe der Arbeit auf eine andere Anwendung übergehen, wird die **Dr.Web Firewall** deaktiviert. In dem Benachrichtigungsbereich wird dabei die entsprechende Warnmeldung angezeigt. Um **Dr.Web Firewall** wieder zu aktivieren, brauchen Sie nur auf diese Warnmeldung zu klicken.

Besonderheiten der Nutzung

Dr.Web Firewall wird auf Basis der VPN-Technologie für Android realisiert und kann demgemäß funktionieren, ohne dass Superuser-Rechte (root) dafür benötigt werden. Die **Dr.Web Firewall** kann also auf einem beliebigen Gerät benutzt werden, sofern es unter Android 4.0 oder höher läuft. Es bestehen aber bestimmte Einschränkungen beim Realisieren der VPN-Technologie unter Android:

- VPN kann zu jedem Zeitpunkt nur von einer Anwendung auf dem Gerät benutzt werden. Wenn also die Anwendung VPN aktiviert, öffnet sich dabei ein Fenster mit der Anforderung an Benutzer, VPN für diese Anwendung zu erlauben. Wenn der Benutzer es erlaubt, beginnt die Anwendung, VPN zu verwenden. Dabei aber wird VPN für eine andere Anwendung, die bisher VPN verwendete, verboten. Diese Anforderung wird beim ersten Aktivieren der **Dr.Web Firewall** sowie nach jedem Neustart angezeigt. Darüber hinaus kann diese Anforderung angezeigt werden, wenn andere Anwendungen VPN-Zugang beantragen. Die Verwendung von VPN wird also zwischen mehreren Anwendungen zeitlich verteilt und die Firewall kann nur dann funktionieren, wenn sie über alle VPN-Rechte verfügt.
- ein anderes Merkmal, das mit dem Einsatz der VPN-Technologie in Verbindung steht, ist die Option der **Dr.Web Firewall**, anhand der nur die Verbindungen zu externen Netzwerken (Internet) blockiert werden. Die Verbindungen innerhalb eines lokalen Netzwerks können nicht blockiert werden. Es besteht also keine Gefahr, dass die Verbindungen im Heimnetzwerk des Benutzers blockiert werden.

Die VPN-Technologie für Android dient nur zur Realisierung der Firewall-Funktionen. Es wird dabei kein VPN-Tunnel eingerichtet, der Internet-Traffic wird nicht verschlüsselt.

Mobiles Internet einschränken

Mit Hilfe der **Dr.Web Firewall** können Sie die Grenze bei der Nutzung des mobilen Internets festlegen.

1. Um die Option für die Einschränkung des mobilen Internets zu aktivieren/deaktivieren, navigieren Sie zu **Mobiles Internet einschränken** auf der Registerkarte **Allgemein** im Einstellungsbildschirm der Firewall (s. Abbildung 13).
2. Beim Aktivieren dieser Option müssen Sie die Grenze für mobilen Datenverkehr setzen (in Megabytes oder Gigabytes). Sie können den Zeitraum festlegen, innerhalb dessen die Einschränkung gültig ist: ein Tag, eine Woche oder ein Monat.
3. Gegebenenfalls geben Sie das verbrauchte Traffic-Volumen ab Beginn der festgelegten Einschränkung der Internetnutzung an:
   - wenn ein Tag als die Dauer der Einschränkung festgelegt wurde, wird die Zeit ab 00:00 des laufenden Tages berechnet;
   - wenn eine Woche als die Dauer der Einschränkung festgelegt wurde, wird die Zeit ab 00:00 des laufenden Tages berechnet;
   - wenn ein Monat als die Dauer der Einschränkung festgelegt wurde, wird die Zeit ab 00:00 des ersten Tages des laufenden Kalendermonats berechnet.

Wenn die Einschränkung der Nutzung des mobilen Internets aktiviert wird, wird ein Diagramm mit Information zum verbleibenden Traffic auf der Registerkarte **Allgemein** im Einstellungsbildschirm der Firewall angezeigt. Daneben finden Sie auch die Angaben zur festgelegten Traffic-Grenze und einen Counter, der die Zeit bis zum Ablauf der Einschränkung rückwärts zählt (s. Abbildung 14).

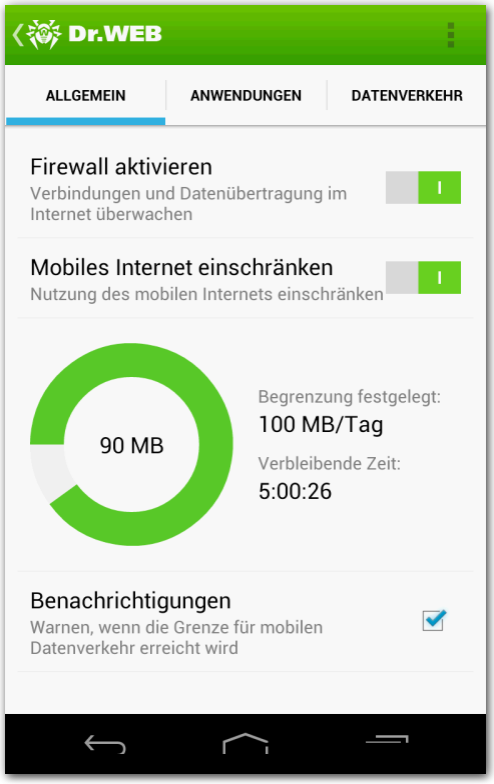


Abbildung 14. Einstellungsbildschirm der Firewall mit aktivierter Option zur Einschränkung des mobilen Internets.

Beim Einschränken des mobilen Datenverkehrs ist eine geringe Überschreitung von max. 4 KB erlaubt.

Benachrichtigungen

Sie können die Benachrichtigungen über das Erreichen der festgelegten Grenze für mobilen Datenverkehr konfigurieren. Dazu markieren Sie das Kontrollkästchen bei **Benachrichtigungen** auf der Registerkate **Allgemein** im Einstellungsbildschirm der Firewall(s. Abbildung 13).

Anwendungsdatenverkehr behandeln

Die **Dr.Web Firewall** ermöglicht es, die Behandlung des Internetdatenverkehrs auf Anwendungsebene zu konfigurieren, sodass Sie den Zugriff bestimmter Programme und Prozesse auf die Netzwerkressourcen überwachen können. Die Informationen zum Internetdatenverkehr, der von den auf Ihrem Gerät installierten Anwendungen verwendet wird, finden Sie auf der Registerkarte **Anwendungen** im Einstellungsbildschirm der Firewall. Hier können Sie auch die Zugriffsregeln auf die Netzwerkressourcen für die Anwendungen einstellen (s. Abbildung 15).

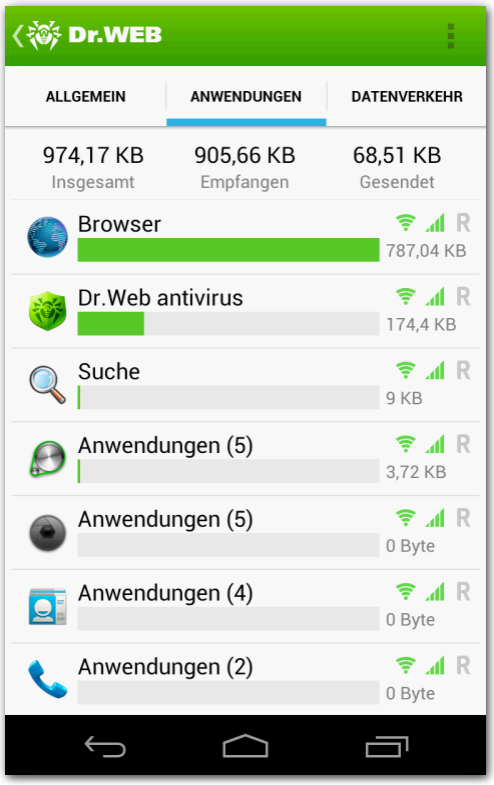


Abbildung 15. Einstellungsbildschirm der Firewall. Registerkarte Anwendungen.

Auf der Registerkarte **Anwendungen** wird die Gesamtzahl der im Netzwerk übertragenen Daten sowie das Volumen des empfangenen und gesendeten Traffics angezeigt.

Nachstehend finden Sie eine Liste der Anwendungen (und Anwendungsgruppen) mit Angabe des verbrauchten Internettraffics für jede davon. Um die Liste aller auf dem Gerät installierten Anwendungen, einschließlich der Anwendungen, deren Traffic-Verbrauch null beträgt, anzeigen zu lassen, aktivieren Sie das Kontrollkästchen **Alle Anwendungen** im Menü auf der Registerkarte **Anwendungen**.

Für jede Anwendung können Sie die Nutzung von Wi-Fi, mobilem Internet und Internet im Roaming anhand der entsprechenden Optionen, die rechts von dem Anwendungsnamen untergeordnet sind, erlauben/verbieten.

Um detaillierte Informationen zur Internetnutzung durch eine Anwendung (Anwendungsgruppe) in der Liste einzusehen, klicken Sie darauf. Im geöffneten Fenster sind folgende Optionen verfügbar:

- die Nutzung von Wi-Fi, mobilem Internet und Internet im Roaming der Anwendung (Anwendungsgruppe) erlauben/verbieten;
- das Protokoll der Anwendung (Anwendungsgruppe) einsehen;
- die Statistik für die Nutzung des Internetdatenverkehrs durch diese Anwendung (Anwendungsgruppe) einsehen;

- die Regeln für Behandlung von Verbindungen für ausgewählte Anwendung (Anwendungsgruppe) einstellen.

Statistik zur Nutzung des Internet-Datenverkehrs

Auf dem Bildschirm mit detaillierten Informationen zum Datenverkehr einer Anwendung (Anwendungsgruppe) können Sie die grafisch dargestellte Statistik zur Internetnutzung durch diese Anwendung einsehen (s. Abbildung 16).

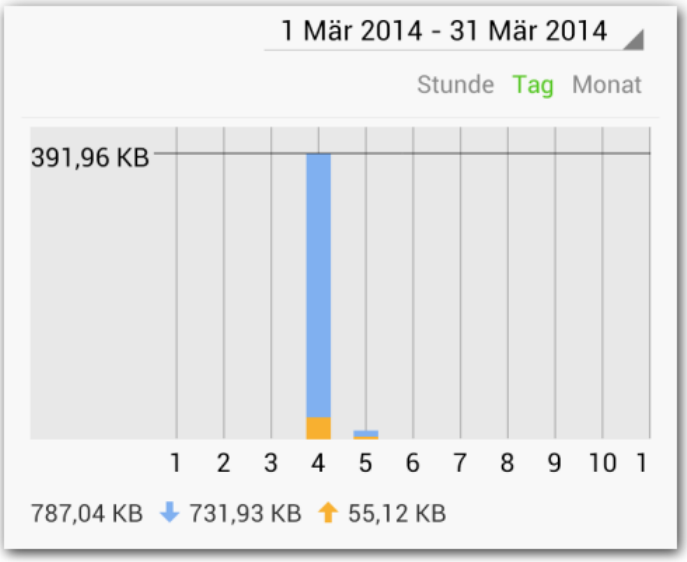


Abbildung 16. Statistik zur Nutzung des Internettraffics durch die Anwendung.

Gelb ist der ausgehende Datenverkehr, blau ist der eingehende Datenverkehr im Diagramm markiert. Unter dem Diagramm sind die Zahlenwerte für verbrauchten Traffic (gesamt, ausgehend und eingehend) angeführt.

Beim Einsehen der Statistiken zur Nutzung des Internet-Datenverkehrs können Sie folgende Aktionen durchführen:

- einen Zeitabstand zum Einsehen der Statistik in der entsprechenden Lise auswählen. Es stehen Ihnen die statistischen Daten für laufenden Tag, letzte Woche, laufenden Monat, vorherigen Monat zur Verfügung. Sie können auch einen Zeitabstand selbständig definieren. Dazu geben Sie das Anfangs- und Endedatum an;
- innerhalb des ausgewählten Zeitabstandes können die Statistiken nach Stunden, Tagen oder Monaten angezeigt werden.

Statistik bereinigen

Gegebenenfalls können Sie die ganze Statistik zum Betrieb der Firewall bzw. die Statistik für einzelne Anwendungen leeren.

Um die Statistik für alle Anwendungen zu löschen:

1. Auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall (s. Abbildung 13) wählen Sie die Option **Bereinigen** im Menü aus.
2. In dem geöffneten Fenster aktivieren Sie das Kontrollkästchen **Statistik bereinigen**. Klicken Sie auf **OK**.

Um die Statistik für eine bestimmte Anwendung zu löschen:

1. Auf der Registerkarte **Anwendungen** im Einstellungsbildschirm der Firewall (s. Abbildung 15) wählen Sie die Anwendung, deren Statistik zu löschen ist.
2. Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung wählen Sie die Option **Bereinigen** im Menü aus.
3. In dem geöffneten Fenster aktivieren Sie das Kontrollkästchen **Statistik für diese Anwendung bereinigen**. Klicken Sie auf **OK**.

Verbindungsregeln

Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung (Anwendungsgruppe) können Sie auch die Regeln für die Verbindung dieser Anwendung zu bestimmten IP-Adressen und Ports festlegen.

Einen Regelsatz erstellen

1. Um eine Regel zu erstellen, klicken Sie auf **Regel hinzufügen**. Sie können erlaubende und verbietende Regeln je nach Auswahl einer entsprechenden Option im Bereich **Verbindungsregeln** hinzufügen:
   - wenn **Verbindungen in der Liste sperren** ausgewählt ist, wird eine verbietende Regel hinzugefügt.
   - wenn **Nur Verbindungen in der Liste erlauben** ausgewählt ist, wird eine erlaubende Regel hinzugefügt
2. Im Fenster zur Regelerstellung im Feld **IP-Adresse** geben Sie eine gültige IP-Adresse (im Format a.b.c.d), IP-Adressenbereich (im Format a1.b1.c1.d1-a2.b2.c2.d2) oder das ganze Netzwerk (im Format a.b.c.0/n, wobei n - eine Zahl von 1 bis 32) an oder lassen Sie das Feld leer (in diesem Fall müssen Sie den Verbindungsport unbedingt festlegen). Im Feld **Port** geben Sie die Nummer eines gültigen Ports an oder lassen Sie das Feld leer (in diesem Fall müssen Sie die IP-Adresse der Verbindung unbedingt festlegen). Wenn eines der Felder leer geblieben ist, gilt die Regel für beliebige IP-Adressen oder Ports. Klicken Sie auf **OK**, um erstellte Regel zu speichern.
3. Um eine bestehende Regel zu bearbeiten, klicken Sie auf diese Regel in der Liste und halten Sie diese gedrückt, dann klicken Sie auf **Editieren**.
4. Um eine Regel zu löschen, klicken Sie in der Liste darauf und halten Sie diese gedrückt, dann klicken Sie auf **Löschen**.

Darüber hinaus können Sie erlaubende und verbietende Regeln beim Einsehen der Anwendungsprotokolle bzw. der Liste von laufenden Verbindungen.

Eingehende Verbindungen

Das Kontrollkästchen **Eingehende Verbindungen erlauben** im Menü auf dem Bildschirm mit Informationen zum Anwendungstraffic ermöglicht es Ihnen, eingehende Verbindungen von der Prüfung durch die Firewall auszunehmen. Die Information zu den Verbindungen, die von beliebigen Remote-Adressen mit dem durch diese Anwendung geöffneten Port initiiert wurden, wird in dem Anwendungsprotokoll und der Statistik zum Betrieb der Firewall nur teilweise angeführt. Des Weiteren können beliebige Verbindungen mit diesen Adressen von der Prüfung durch die Firewall auch für andere Anwendungen ausgenommen werden. Ein solcher Modus ist nicht sicher, und es wird nicht empfohlen, diesen im allgemeinen Fall zu verwenden.

Es ist sinnvoll, die eingehenden Verbindungen zu erlauben, wenn die Deaktivierung der Firewall auf keine andere Weise verhindert werden kann. Zum Beispiel, wenn ein Server, der Verbindungen von externen Netzwerken akzeptiert, auf dem Gerät konfiguriert ist.

Aktuelle Aktivität der Netzwerkverbindungen

Auf der Registerkarte **Datenverkehr** im Einstellungsbildschirm der Firewall (s. Abbildung 13) wird eine

Liste der Verbindungen, die durch die auf dem Gerät installierten Anwendungen initiiert wurden, in Echtzeit angezeigt. Um detaillierte Information zu Verbindungen einer Anwendung (IP-Adressen und Ports der Verbindungen sowie das Volumen des gesendeten/empfangenen Datenverkehrs) anzeigen zu lassen, klicken Sie in der Liste darauf.

Sie können erlaubende bzw. verbietende Regeln für die Anwendungen in der Liste erstellen. Klicken Sie und halten Sie die Verbindung in der Liste gedrückt, danach wählen Sie die entsprechende Option aus:

- **Erlaubende Regel hinzufügen**, um eine Regel zu erstellen, die Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port erlaubt;
- **Verbietende Regel hinzufügen**, um eine Regel zu erstellen, die alle Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port sperrt.

Ereignisse registrieren

Das Programm registriert die Ereignisse, die mit dem Betrieb der **Dr.Web Firewall** verbunden sind. Sie können die gesamte Liste der Ereignisse oder nur die Ereignisse, die mit Nutzung des Internet-Traffics durch einzelne Anwendungen verbunden sind, einsehen.

Protokoll der Dr.Web Firewall

Um die Liste aller Ereignisse, die mit dem Betrieb der **Dr.Web Firewall** verbunden sind, anzeigen zu lassen, wählen Sie die Option **Protokoll** im Menü auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall aus (s. Abbildung 13).

Ereignisprotokoll anzeigen lassen

Damit die Suche nach Informationen einfacher wird, können Sie die Sortierung der Einträge und schnelles Scrollen (durch Bewegen eines speziellen grafischen Elementes im rechten Bildschirmbereich) beim Einsehen der Ereignisliste verwenden. Zur Sortierung der Einträge im Protokoll wählen Sie das Sortierungskriterium im Menü auf dem Protokoll-Bildschirm.

Es werden folgende Informationen für jedes Ereignis im Protokoll angezeigt:

- Datum und Zeit der Verbindung (für TCP) bzw. Zeitraum, innerhalb dessen die Datenpakete mit entsprechenden Traffic-Werten empfangen wurden (für UDP). Zum Beispiel: 18/02/2014 2:07:11 - 18/02/2014 2:07:12;
- lokale Adresse und lokaler Port. Zum Beispiel: src: 10.2.3.5:6881;
- eingehender und ausgehender Datenverkehr (in Bytes) bzw. Anzahl der gesperrten Pakete. Zum Beispiel: in:103 out:112 oder blocked packets:1;
- ID einer Anwendung auf dem Gerät, die mit diesem Datenverkehr assoziiert ist (User ID). Zum Beispiel: uid=10071;
- Anzahl an Datenverkehrsstaus (nur für TCP). Zum Beispiel: traffic jam=0. Datenverkehrsstau ist eine Situation, wenn das Client-Programm den TCP-Pufferspeicher rechtzeitig nicht entladen kann. Dabei entsteht ein Stau, durch den die Datenübertragung im Netzwerk langsamer werden kann.

Protokoll bereinigen

Um alle Ereignisse, die mit dem Betrieb von **Dr.Web Firewall** verbunden sind, aus der Liste zu löschen, müssen Sie wie folgt vorgehen:

1. Auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall (s. Abbildung 13) wählen Sie die Option **Bereinigen** im Menü aus:
2. Im geöffneten Fenster aktivieren Sie das Kontrollkästchen **Protokoll bereinigen**. Klicken Sie auf **OK**.

Protokollgröße

Standardgemäß beträgt die maximale Größe der Protokolldatei 5 MB. Um die maximale Größe der Protokolldatei zu ändern, müssen Sie wie folgt vorgehen:

1. Auf einer beliebigen Registerkarte im Einstellungsbildschirm der Firewall (s. Abbildung 13) wählen Sie die Option **Bereinigen** im Menü aus.
2. Im geöffneten Fenster ändern Sie den Wert, der im Feld **Maximale Größe der Protokolldatei** angegeben ist. Klicken Sie auf **OK**.

Anwendungsprotokolle

Um die Liste der Ereignisse einzusehen, die mit den Netzwerkverbindungen einer Anwendung auf Ihrem Gerät verbunden sind, klicken Sie auf **Protokoll** auf dem Bildschirm mit detaillierter Information zum Datenverkehr dieser Anwendung.

Anwendungsprotokoll anzeigen lassen

Alle Ereignisse für eine bestimmte Anwendung sind nach Datum im Protokoll vereinigt. Um die Ereignisliste zu einem bestimmten Datum anzeigen zu lassen, klicken Sie in der Liste darauf. Es werden folgende Informationen zu jedem Ereigniss angezeigt:

- Verbindungszeit (für TCP) oder der Zeitraum, innerhalb dessen die Datenpakete mit entsprechenden Traffic-Werten empfangen wurden (für UDP);
- lokale Adresse und lokaler Port;
- eingehender und ausgehender Datenverkehr (in Bytes) bzw. Anzahl der gesperrten Pakete;

Sie können erlaubende bzw. verbietende Regeln für die Verbindungen im Anwendungsprotokoll erstellen. Klicken Sie und halten Sie die Verbindung in der Liste gedrückt, danach wählen Sie die entsprechende Option aus:

- **Erlaubende Regel hinzufügen**, um eine Regel zu erstellen, die Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port erlaubt;
- **Verbietende Regel hinzufügen**, um eine Regel zu erstellen, die alle Verbindungen der gewählten Anwendung zu entsprechender IP-Adresse und Port sperrt.

Anwendungsprotokoll bereinigen

Um das Anwendungsprotokoll zu bereinigen, müssen Sie wie folgt vorgehen:

1. Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung wählen Sie die Option **Bereinigen** im Menü aus.
2. Im geöffneten Fenster aktivieren Sie das Kontrollkästchen **Protokoll für diese Anwendung bereinigen**. Klicken Sie auf **OK**.

Registrierung von Ereignissen für eine Anwendung deaktivieren

Gegebenenfalls können Sie die Protokollierung für manche Anwendungen deaktivieren. Dafür müssen Sie wie folgt vorgehen:

1. Auf dem Bildschirm mit detaillierter Information zum Datenverkehr der Anwendung wählen Sie die Option **Bereinigen** im Menü aus.
2. Im geöffneten Fenster aktivieren Sie das Kontrollkästchen **Protokollierung für diese Anwendung deaktivieren**. Klicken Sie auf **OK**.

Bei Beseitigung der Sicherheitslücken helfen

Die **Antivirensoftware Dr.Web antivirus** ermöglicht die Diagnose und Analyse der Sicherheit von

Ihrem mobilen Gerät. Die erkannten Sicherheitsprobleme und -lücken lassen sich mit Hilfe einer speziellen Komponente - des **Security Auditor** - beheben. Die Komponente startet automatisch, sobald die Anwendung zum ersten Mal gestartet und die Lizenz registriert wird. Die Anzahl erkannter Probleme wird im Bereich **Hilfe bei Beseitigung der Sicherheitsprobleme** auf dem Hauptbildschirm der Anwendung angezeigt.

Wenn der **Security Auditor** bei der Analyse des Systems keine Sicherheitsprobleme und -lücken entdeckt, wird der entsprechende Bereich auf dem Hauptbildschirm der Anwendung nicht angezeigt.

Mögliche Probleme und deren Beseitigung

Sie können die Liste erkannter Sicherheitsprobleme einsehen (s. Abbildung 17). Tippen Sie dazu auf den Bereich **Hilfe bei Beseitigung der Sicherheitsprobleme** auf dem Hauptbildschirm der Anwendung.

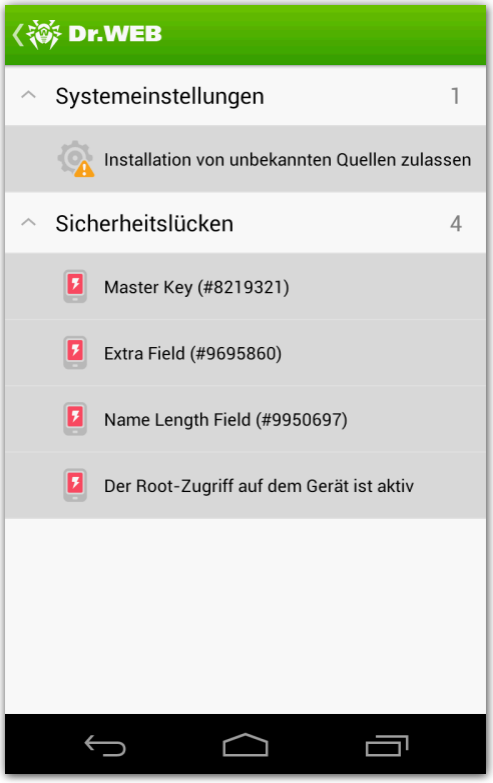


Abbildung 17. Liste der Sicherheitslücken, die im Gerät erkannt wurden.

Mit **Dr.Web antivirus** können folgende Sicherheitsprobleme aufgedeckt werden: Anwendungen mit höchster Priorität bei Behandlung von SMS-Nachrichten, ausgeblendete Geräteadministratoren, Sicherheitslücken und Systemeinstellungen, die Sicherheit Ihres Geräts gefährden. Um detaillierte Informationen zu einem Problem und mögliche Beseitigungswege einzusehen, öffnen Sie die Liste von entsprechender Kategorie und tippen Sie auf das Sicherheitsproblem/-lücke in der Liste.

Anwendungen mit höchster Priorität bei Behandlung von SMS-Nachrichten

Diese Kategorie beinhaltet eine Liste von Anwendungen, die über eine höhere Priorität als die **Dr.Web antivirus** beim Behandeln von SMS-Nachrichten verfügen. Solche Anwendungen können die Funktion von Dr.Web Anti-Theft und Filtern der SMS-Nachrichten sperren, da sie alle eingehenden Nachrichten und Befehle als erste behandeln. In manchen Fällen gehören diese Anwendungen zu Malware und können die Sicherheit Ihres Geräts gefährden.

Sollten Sie gemerkt haben, dass die Nachrichten nicht gefiltert werden bzw. **Dr.Web Anti-Theft** nicht funktioniert, können Sie eventuell versuchen, entsprechende Einstellungen von Anwendungen auf der Liste zu bearbeiten. Die Anwendungen werden aus der Liste der Sicherheitslücken entfernt. Wenn Sie nicht sicher sind, dass diese Anwendungen absolut vertrauenswürdig sind, empfiehlt es sich, diese zu entfernen. Um eine Anwendung zu entfernen, tippen Sie auf **Löschen** in dem Bereich mit detaillierten Informationen zum entstandenen Problem bzw. verwenden Sie das Standardverfahren des Betriebssystems.

Ausgeblendete Geräteadministratoren

Manche Anwendungen werden als Geräteadministratoren aktiviert, dabei aber werden sie in der Liste der Administratoren in den Geräteeinstellungen nicht angezeigt. Diese Anwendungen können mit Standardverfahren des Betriebssystems nicht entfernt werden. Es ist höchstwahrscheinlich, dass solche Anwendungen die Sicherheit Ihres Geräts gefährden können.

Sollten Sie nicht wissen, warum die Anwendung in der Liste der Geräteadministratoren ausgeblendet wird, empfiehlt es sich, diese zu entfernen. Um eine Anwendung zu entfernen, tippen Sie auf **Löschen** in dem Bereich mit detaillierten Informationen zum entstandenen Problem, das mit dieser Anwendung verbunden ist.

Systemeinstellungen

Zu Systemeinstellungen, die die Sicherheit des mobilen Geräts beeinflussen, gehören der Debugging-Modus sowie das Erlaubnis, die Anwendungen aus unbekannten Quellen zu installieren. Des Weiteren kann es gefährlich sein, die in Konflikt stehende Software zu benutzen:

- **USB-Debugging** ist für Entwerfer geeignet. Damit lassen sich die Daten vom Computer auf das mobile Gerät und umgekehrt übertragen sowie die Anwendungen auf dem Gerät installieren, die Logdateien installierter Anwendungen einsehen und diese in manchen Fällen löschen. Falls Sie kein Entwerfer sind und keinen Debugging-Modus verwenden, ist es empfehlenswert, diesen Modus zu deaktivieren. Um zum entsprechenden Bereich der Systemeinstellungen zu wechseln, tippen Sie auf **Einstellungen** in dem Bereich mit detaillierten Informationen zum entstandenen Problem.
- **Installation von Anwendungen aus unbekannten Quellen** ist der Hauptgrund für Verbreitung von Bedrohungen für mobile Geräte. Die nicht von Google Play Store heruntergeladenen Anwendungen können höchstwahrscheinlich gefährlich sein und die Sicherheit Ihres mobilen Geräts gefährden. Um das Risiko bei Installation von nicht sicheren Anwendungen zu reduzieren, empfiehlt es sich, die unbekannten Quellen zu verbieten. Um zum entsprechenden Bereich der Systemeinstellungen zu wechseln, tippen Sie auf **Einstellungen** im Bereich mit detaillierten Informationen zu diesem Problem. Weiterhin ist es empfehlenswert, alle installierten Anwendungen auf Bedrohungen zu scannen. Vor Prüfungsbeginn stellen Sie sicher, dass die **Virendatenbanken** von **Dr.Web** aktualisiert sind.
- **Software-Konflikte**. Durch die Nutzung der in Konflikt stehenden Software, u.a. Browser, die durch den URL-Filter Cloud Checker nicht unterstützt werden, wird die Sicherheit des mobilen Geräts beeinträchtigt. Bei der Nutzung solcher Browser ist der Benutzer vor unerwünschten und schädlichen Web-Ressourcen nicht geschützt. Aus diesem Grund wird es empfohlen, den integrierten Android-Browser als Default-Browser einzustellen und zu benutzen, Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser bzw. Boat Browser Mini.

Sicherheitslücken

Mit **Dr.Web antivirus** können solche Sicherheitslücken wie Master Key (#8219321), Extra Field (#9695860) und Name Length Field (#9950697) im System des mobilen Endgeräts aufgedeckt werden. Mittels dieser Sicherheitslücken können die böswilligen Benutzer den Programmcode manchen Anwendungen hinzufügen, ohne dass deren kryptographischen Signaturen geändert werden. Eine Folge davon ist, dass diese Anwendungen Funktionen, die die Sicherheit des Geräts gefährden werden, ausführen können. **Dr.Web antivirus** entdeckt auch die Heartbleed-Sicherheitslücke im System. Es ist ein Fehler in der kryptographischen OpenSSL-Software, der es den Böswilligen ermöglicht, den Zugriff auf die vertraulichen Angaben des Benutzers zu erhalten.

Wenn eine oder mehrere der genannten Sicherheitslücken entdeckt werden, überprüfen Sie, ob die Updates für das Betriebssystem Ihres Geräts auf der Website des Herstellers vorhanden sind. Die Sicherheitslücken können in neuen Versionen bereits behoben werden. Sollten keine Updates verfügbar sein, empfiehlt es sich, die Anwendungen nur von vetrauenswürdigen Quellen zu installieren.

Weiterhin kann das Gerät durch unterschiedliche Typen der Bedrohungen gefährdet werden, wenn es gerootet ist, d.h. Änderungen vorgenommen wurden, welche mit Erlangen der Superuser-Rechte verbunden sind. Dadurch können die Systemdateien geändert bzw. gelöscht werden und das Gerät wird funktionsunfähig. Wenn Sie selbständig diese Änderungen vorgenommen haben, empfiehlt es sich, sie rückgängig zu machen. Wenn der Root-Zugriff auf Ihrem Gerät technisch bedingt ist bzw. zur Lösung bestimmter Aufgaben benötigt wird, geben Sie besonders acht, wenn Anwendungen aus unbekannten Quellen installiert werden.

Betriebsmodus wählen

Wenn Sie **Dr.Web antivirus** von der Website von **Doctor Web** installiert haben, können Sie das installierte Programm für Ihre Arbeit im Netzwerk, das über **Dr.Web Verwaltungscenter** kontrolliert wird, oder auch für die Verbindung zum Antivirus-Dienst **Dr.Web® AV-Desk**, der von Ihrem IT-Anbieter zur Verfügung gestellt wird, nutzen. Für den Virenschutz mit zentraler Verwaltung brauchen Sie keine zusätzlichen Plugins zu installieren bzw. das installierte **Dr.Web antivirus** Programm zu deinstallieren.

Die von Google Play installierte Version von **Dr.Web antivirus** verfügt über keinen zentral verwalteten Schutzmodus.

Zentral verwalteten Schutzmodus konfigurieren

1. Kontaktieren Sie den Administrator des Antivirus-Netzwerks des Unternehmens bzw. des IT-Anbieters, um Parameter für die Verbindung zum zentral verwalteten Virenschutz-Server zu erhalten.
2. Auf dem Hauptbildschirm der Anwendung rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen**.
3. Um eine Verbindung zum Antivirus-Netzwerk des Unternehmens bzw. zum Antivirus-Dienst, der von Ihrem IT-Anbieter zur Verfügung gestellt wird, aufzubauen, setzen Sie ein Häkchen bei **Dr.Web Agent** im **Modus**-Bereich auf dem Bildschirm **Dr.Web - Einstellungen** (s. Abbildung 6).

   Im zentral verwalteten Schutzmodus wird manueller Start sowie Konfigurieren von Updates gesperrt. Darüber hinaus können manche Einstellungen von **Dr.Web antivirus**, insbesondere die Möglichkeit, den permanenten Schutz sowie Systemprüfung auf Anforderung zu verwalten, nach Sicherheitslinien des Unternehmens bzw. gemäß Liste der bezahlten Leistungen geändert bzw. gesperrt werden. Die Schlüsseldatei wird für die Arbeit in diesem Modus vom zentral verwalteten Virenschutz-Server automatisch übermittelt. Ihr persönlicher Lizenzschlüssel wird dabei nicht verwendet.

4. Bei Aktivierung des zentral verwalteten Schutzmodus werden die zuletzt genutzten Verbindungseinstellungen wiederhergestellt. Wenn Sie eine Verbindung zum Server zum ersten Mal herstellen bzw. die Verbindungseinstellungen geändert wurden, gehen Sie wie folgt vor:
   - Geben Sie die IP-Adresse des zentral verwalteten Virenschutz-Servers ein, die vom Administrator des Antivirus-Netzwerks vergeben wird. Gegebenenfalls geben Sie auch den Port, über den die Verbindung zum Server erfolgt, durch einen Doppelpunkt von der IP-Adresse getrennt an.
   - Geben Sie zusätzliche Parameter für Autorisierung der Workstation an: ID (der Ihrem mobilen Gerät zur Registrierung auf dem Server vergeben wird) und Passwort. Die angegebenen Parameterwerte werden gespeichert, somit brauchen Sie nicht, sie bei wiederholter Verbindung zum Server erneut einzugeben.
   - Drücken Sie die **Verbinden**-Taste.

   Die Verbindungseinstellungen zum zentral verwalteten Virenschutz-Server sind in der Datei install.cfg enthalten, die vom Administrator des Antivirus-Netzwerks zur Verfügung gestellt wird. Um die Datei zu nutzen, verschieben Sie diese in ein Verzeichnis der ersten Verschachtelungsebene auf der SD-Karte. Wenn die Datei auf das Gerät heruntergeladen wurde, werden die Felder zur Eingabe der Verbindungsparameter zum Server automatisch ausgefüllt.

   Sollten die Verbindungsparameter zum Beispiel geändert werden, können Sie gegebenenfalls die gespeicherten Parameter zurücksetzen. Dazu navigieren Sie ins Anwendungsmenü auf dem Bildschirm mit Verbindungseinstellungen und wählen Sie hier die Option **Verbindungseinstellungen zurücksetzen**.

Sollte beim Aufbau der Verbindung ein Fehler mit dem Inhalt **Nicht unterstützte Option in den Server-Einstellungen. Prüfen Sie die Konfiguration des Servers und stellen Sie sicher, dass die Parameter "Encryption" und "Compression" nicht den Wert "Yes" haben** auftreten, wenden Sie sich bitte zur Beseitigung des Problems an den Administrator des Antivirus-Netzwerkes. Sind Sie selbst der Administrator des Antivirus-Netzwerkes, überprüfen Sie bitte die Einstellungen und versuchen Sie erneut, die Verbindung aufzubauen.

Offline-Modus konfigurieren

1. Auf dem Hauptbildschirm der Anwendung rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen**.
2. Um in den Offline-Modus des Antivirus-Programms zu wechseln, wählen Sie das Häkchen bei **Dr.Web Agent** im **Modus**-Bereich auf dem Bildscirm **Dr.Web - Einstellungen** ab (s. Abbildung 6).

   Bei Aktivierung des Offline-Modus werden alle Einstellungen des Antivirus-Programms, die vor Wechseln in den zentral verwalteten Schutzmodus festgelegt wurden, bzw. die Default-Einstellungen wiederhergestellt. Es wird auch Zugriff auf alle Funktionen von **Dr.Web antivirus** wieder gestattet.

3. Um im Offline-Modus arbeiten zu können, wird eine gültige persönliche Schlüsseldatei benötigt. Der vom zentral verwalteten Virenschutz-Server automatisch übermittelte Schlüssel kann in diesem Modus nicht verwendet werden. Gegebenenfalls können Sie persönliche Schlüsseldatei erhalten bzw. aktualisieren.

Liste verfügbarer Anwendungen einstellen

Wenn Sie Administrator des Antivirus-Netzwerks sind, können Sie eine Liste von Anwendungen, die für Benutzer des Antivirus-Netzwerks auf ihren Geräten verfügbar sein werden, einstellen. Dafür gehen Sie wie folgt vor:

1. Auf dem Hauptbildschirm der Anwendung öffnen Sie den **Administrator**-Bereich.
2. Im Bereich **Dr.Web - Kontrolle von Anwendungen** wählen Sie Anwendungen aus, die für Benutzer des Antivirus-Netzwerks auf ihren mobilen Geräten verfügbar sein werden.
3. Drücken Sie die Taste **Ausgewähltes erlauben**.

Kurz-URL-Dienst

In manchen Fällen, z.B. bei begrenzter Anzahl von Zeichen in SMS-Nachrichten und sozialen Netzwerken, können kurz-URLs benötigt werden. **Dr.Web antivirus** ermöglicht es, Links zu kürzen und deren Inhalte mittels eines speziellen Kurz-Link-Dienstes zu überprüfen. Somit werden die Benutzer vor Virenbedrohungen geschützt.

Kurz-URL-Dienst nutzen

Um eine URL zu überprüfen und zu kürzen, gehen Sie wie folgt vor:

1. Markieren Sie die URL, die Sie überprüfen und kürzen möchten, und benutzen Sie die Browser-Funktion "Link senden".
2. Im geöffneten Menü wählen Sie den Punkt **URL verkürzen**. Die Webseite unter angegebener URL wird auf Bedrohungen gescannt. Wenn die Webseite sicher ist, wird die URL gekürzt und in die Zwischenablage kopiert. Sollte die Webseite Sicherheitsbedrohungen beinhalten, wird entsprechende Warnung von dem Dienst angezeigt.

Anhang

Anhang A. Technischer Support

Bei Problemen mit der Installation der Produkte nutzen Sie folgende Möglichkeiten, bevor Sie sich an den technischen Support wenden:

- Lesen Sie Produktinformationen und Anleitungen unter http://download.drweb.com/doc/ durch
- Lesen Sie Häufig gestellte Fragen unter http://support.drweb.com/show_faq/ durch
- Besuchen Sie Dr.Web Foren unter http://forum.drweb.com/

Wenn Sie nicht geschafft haben, das Problem zu lösen, dann können Sie eine Web-Form einer Frage im Abschnitt unter http://support.drweb-av.de/support_wizard/ ausfüllen.

Die nächste Vertretung von **Doctor Web** und alle notwendigen Informationen über unser Unternehmen können Sie unter http://company.drweb-av.de/contacts/offices/ finden.

Schlagwortregister

A

Aktionen bei Bedrohungen 29
Aktionen für Bedrohungen
  akustische Benachrichtigungen 28
  Quarantäne 34
Aktualisierung
  automatische Aktualisierung 34
  Einstellungen 34
Antispam 30
Antivirenschutz 25
Antivirensoftware Dr.Web antivirus
  Lösen der Sicherheitsprobleme 51
Antivirus-Netzwerk 55
Anwendungen
  Datenverkehr 48, 49
  eingehende Verbindungen 49
  Statistik 48
  Verbindungsregeln 49
Arbeitsbeginn 18
ausgeblendete Geräteadministratoren 51
Autostart-Dateien 25, 26

B

Bedrohungen
  Bearbeiten 29
  Sperr-Software 29
  Systemanwendungen 29
Benachrichtigungen 20
  mobiles Internet 45
Benachrichtigungsleiste 20
benutzerdefinierte Prüfung 26
Betriebsmodus 55
Blacklist 31

C

Cloud Checker 42
  Einstellungen 42
  Kategorien von Websites 42

D

Datei an das Virenlabor senden 26, 28, 34
Deinstallation des Programms 15, 17
Demo 10
Demoschlüsseldatei 9
Dr.Web Anti-Theft 36
  Anmeldung 37
  Deaktivierung 37, 42
  Einstellungen 37, 39
  Einstellungsassistent 37
  Freundesliste 40
  Passwort 37
  Passwort zurücksetzen 42
  SMS-Befehle 41
  Vertrauenswürdige SIM-Karten 39
Dr.Web antivirus 6, 15, 17
  Aktionen 28
  Aktualisierung 34
  Arbeitsbeginn 18
  Benachrichtigungen 20
  Betriebsmodus 55
  Blacklist 31
  Cloud Checker 42
  Deinstallation 15
  Dr.Web Anti-Theft 36, 37, 39, 40, 41, 42
  Einstellungen 23
  Einstellungen exportieren 23
  Einstellungen importieren 23
  Einstellungen zurücksetzen 23
  Ereignislog 35
  Filtern 30, 31, 33
  Filterprofile 32
  Funktionen 7, 23
  Installation 15
  Lizenz 8
  Mein Dr.Web 21
  Oberfläche 18
  Quarantäne 34
  Scanner 26
  Schlüsseldatei 8
  Spamschutz 30
  SpIDer Guard 25
  Start 18
  Statistik 35
  Systemanforderungen 15
  URL kürzen 57
  Virenschutz 25
  Wächter 25
  Widgets 19
Dr.Web antivirus Antivirus
  Dr.Web Firewall 43
Dr.Web Firewall 43

Schlagwortregister

Dr.Web Firewall 43
  Anwendungsdatenverkehr 48, 49
  Anwendungstraffic 47
  eingehende Verbindungen 49
  Ereignisse registrieren 50, 51
  Internet-Traffic 49
  mobiles Internet einschränken 45
  Netzwerkverbindungen 49
  Protokoll 50
Dr.Web Icon 25

E

Einstellungen exportieren 23
Einstellungen importieren 23
Einstellungen zurücksetzen 23
Ereignislog 35

F

Fehlalarm 26, 28, 34
Filter 31
  Blacklist 31
  des Benutzers 32
Filtermodus 31
Filtern 30
  Blacklist 31
  Gesperrte einsehen 33
  Modus 31
  Profile 32
  von Anrufen 30
  von Nachrichten 30
Filterprofile 32

G

Gesperrte einsehen 33
Google Play 15, 17

H

Hilfe
  Lösen der Sicherheitsprobleme 51

I

Installation des Programms 15
Internet-Datenverkehr
  von Anwendungen 48
Internet-Traffic
  mobil 45
  von Anwendungen 47, 49

L

Links kürzen 57
Lizenz
  Aktualisierung 13
  Aus der Datei laden 12
  Erhalten 10
  Erwerb 10
  Gültigkeit 9
  Herunterladen 10
  Nutzung 12
  Registrierung der Seriennummer 12
  Verlängerung 13
Lizenz Kaufen 10
Lizenzierung 8
Lizenzschlüsseldatei 9
Lösen der Sicherheitsprobleme
  ausgeblendete Geräteadministratoren 51
  Priorität bei Behandlung der SMS-Nachrichten 51
  root-Zugriff 51
  Sicherheitslücken 51
  Systemeinstellungen 51

M

Market 15, 17
mobiles Internet
  Benachrichtigungen 45
  Nutzungsgrenze 45

N

Netzwerkverbindungen
  aktuelle Aktivität 49

O

Oberfläche 18

P

permanenter Schutz 25
persönlicher Bereich Mein Dr.Web 21
Priorität bei Behandlung der SMS-Nachrichten 51
Programmeinstellungen
  Aktualisierung 34
  Dr.Web Anti-Theft 37, 39
  Einstellungen zurücksetzen 23
  Export 23

Schlagwortregister

Programmeinstellungen
- Import 23
- Scanner 26
- URL-Filter 42
- Vertrauenswürdige SIM-Karten 39
- Wächter 25

Programmfunktionen 7
Protokoll
- von Anwendungen 51
- von Dr.Web Firewall 50

Prüfung
- benutzerdefiniert 26
- schnell 26
- vollständig 26

Q

Quarantäne
- Aktionen für Bedrohungen 34
- Größe 34

R

Ransomware 29
Registrierung der Seriennummer 12
root-Zugriff 51

S

Scanner
- benutzerdefinierte Prüfung 26
- Einstellungen 26
- schnelle Prüfung 26
- Statistik 26
- vollständige Prüfung 26

Schlüsseldatei 9
- Aktualisierung 13
- Aus der Datei laden 12
- Erhalten 12
- Erwerb 10
- Gültigkeit 9
- Herunterladen 10
- Nutzung 12

schnelle Prüfung 26
Schutzstatus 18
Sicherheitslücken 51
Spamschutz 30
Sperr-Software 29
SpIDer Guard
- Aktivierung 25
- Einstellungen 25
- Statistik 25

Start des Programms 18
Statistik 35
- des Anwendungsdatenverkehrs 48
- Scanner 26
- Wächter 25

Symbole 6
Systemanforderungen 15
Systemeinstellungen 51

U

URL-Filter 42

V

Verbindungsregeln 49
Vertrauenswürdige SIM-Karten 39
Virendatenbanken
- Aktualisierung 34

Virenschutz 25
vollständige Prüfung 26

W

Wächter
- Aktivierung 25
- Einstellungen 25
- Statistik 25

Widgets 19

Z

zentral verwalteter Schutz 55

© Doctor Web, 2014